

Consistency of Quine's New Foundations using nominal techniques

Murdoch J. Gabbay, <http://www.gabbay.org.uk>

We build a model in nominal sets for TST+; typed set theory with typical ambiguity. It is known that this is equivalent to the consistency of Quine's New Foundations.

The model is in the spirit of a representation theorem and is built out of points, in the sense of filters of predicates. The model is *absolute*, meaning that variables are interpreted directly as atoms of the nominal theory. Predicates are interpreted as possibly non-equivariant sets of points, and sets are interpreted using nominal atoms-abstraction, which behaves in this context like a semantic counterpart to sets comprehension.

Additional Key Words and Phrases: Set theory, New Foundations, nominal techniques, mathematical foundations

Contents

1	Introduction	3
1.1	How this paper works	3
1.2	Further comments	6
2	Background on nominal techniques	6
2.1	Basic definitions	7
2.1.1	Cardinalities and atoms	7
2.1.2	Permutation actions on sets	9
2.1.3	Nominal sets	10
2.2	Examples	10
2.2.1	Atoms	10
2.2.2	Cartesian product	10
2.2.3	Full function space	10
2.2.4	Small-supported function space	10
2.2.5	Full powerset	11
2.3	The principle of equivariance and two nominal quantifiers	11
2.3.1	Equivariance	11
2.3.2	The New and the Generous quantifiers	12
2.4	Further examples	13
2.4.1	Small-supported powerset	13
2.4.2	Finite powerset	14
2.4.3	Strictly small-supported powerset	14
2.5	The NEW-quantifier for nominal sets	15
2.6	Atoms-abstraction	16
3	Internal predicates	17
3.1	Basic definition	17
3.2	Some useful notation	19
4	The sigma-action	19
4.1	Basic definitions and lemmas	19
4.2	Alpha-equivalence and substitution on \mathbf{elt}	22
4.3	Further nominal algebra properties of the σ -action	23
4.3.1	Property ($\sigma\#$) (garbage collection)	23
4.3.2	σ commutes with atoms-concretion	24
4.3.3	σ commutes with itself: the 'substitution lemma'	24

4.3.4	(σid): substitution for atoms and its corollaries	27
5	The denotation of an internal predicate as a set of prepoints	27
5.1	Prepoints and the denotation	28
5.2	The amgis-action on prepoints	30
5.3	Proof that amgis is dual to sigma	31
6	Some sugar, and its properties	33
6.1	Prepoints as maps from internal sets to sets of internal sets	33
6.1.1	The basic definition	33
6.1.2	Syntactic lemmas	34
6.1.3	Semantic lemmas	35
6.2	Operations on internal sets	36
6.2.1	Intersection, complement, and ‘every’ on internal sets	36
6.2.2	Interaction with the sigma-action	37
7	The internal algebraic theory of prepoints	38
7.1	The basic definitions and lemmas	38
7.2	Equalities	39
8	Points	42
8.1	The basic definition	42
8.2	Quantification	43
8.3	Extensionality	45
9	Typed set theory	45
9.1	Formulae of the language of typed set theory	45
9.2	Interpretation for formulae and terms	46
9.3	Properties of the interpretation	47
9.4	The denotation of a formula	49
9.5	Consistency of TST, if points exist	49
9.6	Consistency of TST+, if points exist	50
10	Theories	52
10.1	The basic definition	52
10.2	Deductive closure	53
10.3	Further properties of small theories	54
10.4	The syntactic prepoint	55
10.5	A sanity check	56
10.6	Counting subsets	56
11	Extensionality	57
11.1	We enumerate atoms, internal sets, and pairs of internal sets	58
11.2	Constructing an extensional theory	60
11.2.1	We build an extensional equality theory ext	60
11.2.2	Maximality	62
11.2.3	Deductive closure and consistency	62
11.2.4	Generous naming in ext	63
11.3	Properties of the Herbrand prepoint for ext	65
11.3.1	A simple property	65
11.3.2	Naming atoms	65
11.3.3	Extensionality, using internal predicates	66

11.3.4	Three sets of internal predicates	67
12	Existence of a point	68
12.1	An entailment relation	69
12.1.1	Basic definitions and lemmas	69
12.1.2	Soundness, and a corollary of soundness	70
12.1.3	Cut-admissibility	71
12.2	Small substitutions	71
12.3	We build a maximally consistent set $\text{maxfilt}(\Theta)$	74
12.3.1	Some preliminaries	74
12.3.2	We build the set	75
12.3.3	Consistency of the set	77
12.3.4	Other properties of $\text{maxfilt}(\Theta)$	77
12.3.5	We build a point	79
13	Conclusions	80
13.1	Future work	80
13.2	Key ideas of this paper	81
13.3	More on the use of nominal techniques	82
A	A little more on elements and Leibniz equality	85
B	There are infinitely many internal sets at each level	85

1. INTRODUCTION

Consider the following *false* reasoning: define $x = \{a \mid a \notin a\}$. It is easy to check that $x \in x$ if and only if $x \notin x$. This is Russell’s paradox and is one of the central paradoxes of (naive) set theory.

Zermelo-Fraenkel set theory (**ZF**) avoids paradox by insisting that a be *guarded*; we can only form $\{a \in y \mid a \notin a\}$ where y is already known to be a set. The price we pay for this is that we cannot form ‘reasonable’ sets such as the **universal set** $\{a \mid \top\}$ (the set of all sets) or the set of ‘all sets with 2 elements’, and so on. In ZF, these are *proper classes*.¹

New Foundations (**NF**) avoids paradox by insisting on a stratifiable language [Qui37]. Every variable and term can be assigned a *level*, such that we only form $t \in s$ if $\text{level}(s) = \text{level}(t) + 1$. So $a \in a$ and $a \notin a$ are outlawed because no matter what level i we assign to a , we cannot make i equal to $i + 1$. We can stratify \top so we can still form the universal set in NF, and ‘has 2 elements’ is also stratifiable.

Excellent discussions are in [For95] and [Hol98], and a clear summary with a brief but well-chosen bibliography is in [For97].

However, at the time of writing we know of no published proof of consistency for NF (relative e.g. to ZF). This has been the situation since NF was introduced in 1937 in [Qui37].

This paper presents what the author believes to be a full proof of the consistency of NF.

Note that this is a paper *about* NF; it is not a paper *in* NF. Familiarity with NF, TST+, or TZT+ as reasoning systems and foundations of mathematics, with all their unique and special features, is not relevant to understanding this paper.

1.1. How this paper works

This paper has many ‘moving parts’ so we will attempt to give the reader some overall feeling for how the proofs fit together. What follows is not intended as an exhaustive description of the technical detail.

First, NF is equiconsistent with TST+ [Spe62]. The proof in this paper is for consistency of TST+; consistency of NF is a corollary.

¹A nice historical account of Russell’s paradox is in [Gri04]. For ZF set theory, see e.g. [Jec06].

The syntax of TST+ is as follows (see Figure 5 and Subsection 9.1):

$$\begin{aligned} \phi &::= \perp \mid \phi \Rightarrow \phi \mid \forall a. \phi \mid s = s \mid s \in s \\ s, t &::= a \mid \{a \mid \phi\} \end{aligned}$$

This is the language of first-order logic extended with base predicates for sets equality $s=t$ and sets epsilon $t \in s$. Also, terms have sets comprehension $\{a \mid \phi\}$.

Axioms are listed in Figures 6 and 7. There is no need to list them here because they are mostly as one might expect of a set theory. There are two non-obvious features:

- Variable symbols a (called *atoms* elsewhere in this paper) are assigned levels, as mentioned above. Levels are natural numbers; levels extend to terms and each term in TST+ syntax has a fixed level (in NF, levels may vary). The reader can think of levels as types. In a related system TZT+ levels are taken to be integers instead of natural numbers. TST+ and TZT+ are equiconsistent and for this discussion, they are interchangeable. ϕ is subject to a *stratification* typing condition that we may only form $t \in s$ in ϕ if $\text{level}(s) = \text{level}(t) + 1$. See Definition 9.2 for details; for now, all we care about is that stratification is an easy-to-express decidable syntactic condition which cuts down on the well-formed terms and predicates.
- TST+ is an extension of TST by *typical ambiguity*. This is discussed in Subsection 9.6; for now, we ignore typical ambiguity.

We continue as follows:

We notice that stratification restricts terms such that the following rewriting procedure normalises with a unique normal form:

$$t \in \{a \mid \phi\} \longrightarrow \phi[a:=t].$$

We can without loss of generality work with normal forms $t \in a$.

This is the origin of, and justification for, the *internal terms* and *internal predicates* of see Subsection 3.1; these are effectively normalised TZT+ terms and predicates. It is interesting that this is the only place our proof really uses stratification: it allows us to define normal forms and so gives us the internal syntax.

A substitution action exists on the internal syntax. When evaluating $(t \in a)[a:=s]$ we calculate $t \in s$ and renormalise. This is the *sigma-action* of Figure 1. Section 4 develops the theory of the sigma-action. There are many inductive proofs involved, but they are all routine, at least in retrospect.

Now we have a high-level choice of how to proceed:

- We could calculate a *truth-set* in TST+. That is, we calculate some set of predicates that is deductively closed and does not contain \perp . This would suffice to prove consistency, but it is very hard to do directly. We will not do it.
- We can construct a compositional semantics for TST+ which assigns \perp a different meaning than \top . A TST+ theory follows by considering the predicates whose meaning is the same as that of \top . This is also very hard, however, nominal techniques and in particular ideas from nominal duality theory [Gab16; GG16] will guide us and make it possible.

We now notice something interesting: the basic predicate of the internal syntax is $t \in a$. We can rewrite this as $a \circ t$, choosing a notation deliberately reminiscent of ‘ a applied to t ’, and we can let a *prepoint* be a set of base predicates of the form $a \circ t$. This is Section 5.

(Alternatively, a prepoint is a function from atoms to sets of terms where a maps to the set of t such that $a \circ t$ is in the prepoint; see Subsection 6.1.)

It might seem that we have accomplished little so far, but in fact we have accomplished a great deal: to apply the nominal duality ideas from [Gab16; GG16] we only require a set with a sigma-action, and we have one with the internal syntax. We can therefore use duality off-the-shelf and we obtain a semantics for first-order logic. The meaning of the internal predicate $t \in a$ is, as it has to be, the set of prepoints that contain $a \circ t$.

Most conveniently this semantics side-steps the impredicativity of $\forall a.\phi$ in TST+ because nominal duality gives us a semantics for universal quantification using the NEW-quantifier \mathbb{I} , off-the-shelf. See Figure 3.

Though we have a semantics for TST+, the price we pay for the convenience mentioned in the previous paragraph is that the semantics is *unsound*; not all the axioms of Figures 6 and 7 are correctly interpreted in the prepoint semantics. In particular we do not have extensionality, and the interpretation of \forall is only partially sound; we do not have $(\forall a.\phi) \Rightarrow \phi[a:=s]$.

This is however not fatal; it simply means that we have too many prepoints. We restrict to semantics using *points*, which are prepoints subject to further well-behavedness conditions—the situation is entirely analogous to how filters and prime filters are sets of predicates subject to further well-behavedness conditions.

Building points is hard, so again we break the problem into smaller and easier pieces:

- Extensionality expresses that $s=t$ should imply $\phi[a:=s] \Leftrightarrow \phi[a:=t]$. In fact it suffices to show that $\forall c.(c \in s \Leftrightarrow c \in t)$ implies $\forall b.(s \in b \Leftrightarrow t \in b)$.
So we build a maximally consistent equality theory *ext* (Definition 11.19) such that any prepoint satisfying *ext* must be extensional in a suitable sense (Corollary 11.26).
It is quite common in non-trivial proofs that at some moment, a small miracle occurs; some piece of ‘good fortune’. The good fortune here is that *ext* which we construct *generously names internal sets*. This is a technical property (see Definition 8.3) which will help us with the next point.
- We now work towards soundness for all properties of \forall , in particular for the axiom $(\forall a.\phi) \Rightarrow \phi[a:=s]$.
Nominal duality assigns \forall a meaning off-the-shelf based on the nominal NEW-quantifier \mathbb{I} , which is convenient in that it shares many important properties with \forall , however its meaning is the *wrong* and *unsound* in general, which is less convenient.
However, for the case of prepoints that generously name internal sets, the off-the-shelf meaning for \forall using \mathbb{I} turns out to be *correct*—intuitively, we can always find a fresh a naming s —so we are fortunate. See Theorem 8.15.

Given the existence of points it is fairly easy to give a compositional sound semantics to TST+. For clarity in this paper we first assume points and give the TST+ semantics; this is Section 9, culminating with Corollaries 9.19 and 9.30. Then we go through the technical details of actually building a point; this is Sections 10 to 12, culminating with Theorem 12.52.

TST plus the axiom of infinity is equiconsistent with Bounded Zermelo set theory, also called MacLane set theory. Since TST+ has consistency greater than TST, we can expect a consistency proof for TST+ to involve the use of a cardinal greater than any powerset in Bounded Zermelo, that is, this cardinal should be an upper bound for the sequence $\#\mathbb{N}, 2^{\#\mathbb{N}}, 2^{2^{\#\mathbb{N}}}, \dots$. This cardinal appears at the start in Subsection 2.1.1. The precise moment in which we use it is in Proposition 11.5, and Proposition 11.30 which depends on it.

There are many other difficulties to overcome or circumvent, and subtleties involved in overcoming or circumventing them; the outline above does not do full justice to the maths to follow. However, we hope it will help the reader to navigate the proof. Further exposition is in the body of the paper.

In summary, an overall high-level outline of our approach is this:

- (1) Use stratification to take normal forms.
- (2) Use nominal duality theory to build a model based on prepoints which is only partially sound.
- (3) Refine it by restricting to points to get a sound model, but we do not yet know that any points exist.
- (4) Construct an extensional equality theory.
- (5) Use it to construct a point.

1.2. Further comments

This paper uses *nominal techniques*, which are based on Fraenkel-Mostowski set theory (**FM**), itself based on Zermelo-Fraenkel set theory with atoms (**ZFA**).²

To the reader familiar with the sets literature, a warning: a related theory NFU (NF with urelements) is known to be consistent and is discussed in detail in [Hol98]. The atoms in ZFA/FM are also sometimes called *urelemente*. These are different: the atoms of this paper are *not* like the urelements of NFU. If the reader sees the word ‘atom’ here, they should think of ZFA/FM atoms and not NFU urelements.

As discussed, this paper proves consistency of TST+ (typed set theory with typical ambiguity) relative to ZFA sets (Zermelo-Fraenkel set theory with atoms); consistency of NF follows since NF is known to be consistent relative to TST+ [Spe62]. More specifically we use nominal techniques in FM sets, and more specifically still this paper builds on nominal theories of posets and representations of first-order logic, most notably from [DG12a; Gab16; GG16]. Whereas those papers were broadly concerned with the theory of *all* models, this paper is concerned with *one specific concrete model* since the existence of one model is all we need for consistency.

A predicate is interpreted as a set of *points*, where a point can be viewed (if we squint) as filters of predicates. The overall design therefore resembles a representation theorem, like the Stone representation for Boolean Algebra (a clear presentation is in [HG98, §34]), though this paper differs from a Stone representation in some significant details, most notably in that it represents TST+ instead of Boolean Algebra.

Readers coming to this paper from a theoretical computer science background—many familiar with nominal techniques may fit this description—can think of the paper as follows: TST+ is a simply-typed λ -calculus enriched with one axiom(-scheme); see Definitions 9.4 and 9.25. It is very simple to specify, if difficult to prove consistent. We prove consistency mostly by nominal inductive proofs, along with a semantic argument based on a suitable notion of filter. To a first useful approximation, if in this paper the reader sees the word *predicate*, they can substitute *element of ground type*; wherever they see the word *set*, they can substitute *lambda-term*; and no harm should come of it.

2. BACKGROUND ON NOMINAL TECHNIQUES

Intuitively, a nominal set is “a set X whose elements $x \in X$ may ‘contain’ finitely many names $a, b, c \in \mathbb{A}$ ”. We may call names *atoms*. The notion of ‘contain’ used here is not the obvious notion of ‘is a set element of’: formally, we say that x has *finite support* (Definition 2.25).

For instance, here are some nominal sets:

— The set of atoms:

$$\{a, b, c, \dots\}.$$

— The set of finite sets of atoms:

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \dots, \{a, b\}, \{a, c\}, \dots\}.$$

— The set of *complements* of finite sets of atoms:

$$\{\mathbb{A}, \mathbb{A} \setminus \{a\}, \mathbb{A} \setminus \{b\}, \mathbb{A} \setminus \{c\}, \dots, \mathbb{A} \setminus \{a, b\}, \mathbb{A} \setminus \{a, c\}, \dots\}.$$

Nominal sets are formally defined in Subsection 2.1, and examples are in Subsections 2.2 and 2.4.

The reader might prefer to read this section only briefly at first, and then use it as a reference for the later sections where these underlying ideas get applied. More detailed expositions are also in [GP01; Gab11; DG12b; Pit13].

In the context of the broader literature, the message of this section is as follows:

²Familiarity with all these different set theories is not necessary to understand the body of the paper. Accounts of them tailored specifically to nominal techniques and mostly compatible with the notations and conventions of this paper, appear in [Gab01; Gab11; DG12b]. A linkage of some ‘nominal’ ideas to some corresponding ‘Fraenkel-Mostowski sets’ ideas is given in [Gab11, Remark 2.22].

- The reader with a category-theory background can read this section as exploring the category of nominal sets, or equivalently the Schanuel topos (more on this in [MM92, Section III.9], [Joh03, A.21, page 79], or [Gab11, Theorem 9.14]).
- The reader with a sets background can read this section as stating that we use Fraenkel-Mostowski set theory (**FM sets**).
A discussion of this sets foundation, tailored to nominal techniques, can be found in [Gab11, Section 10]). FM sets add *urelements* or *atoms* to the sets universe.
- The reader uninterested in foundations can note that previous work [GP01; Gab11; DG12b] has shown that just assuming names as primitive entities in Definition 2.4 yields a remarkable clutch of definitions and results, notably Theorem 2.27 and Corollary 2.28, and Theorems 2.31 and 2.39.

Further discussion is in the body of the paper and in the Conclusions; see in particular Subsections 13.2.

2.1. Basic definitions

2.1.1. Cardinalities and atoms. In this Subsection we introduce atoms (Definition 2.4), single out some useful classes of sets of atoms (Notation 2.6), and note how these classes interact with one another via sets intersection, union, and complement (Lemma 2.11). These definitions and properties are quite simple, but they will be very useful in the rest of this paper.

We will need an infinite hierarchy of atoms to reflect the infinite hierarchy of levels implied by stratification; this will be the i in Definition 2.4.

DEFINITION 2.1. Suppose X is a set. Then:

- We write $\#X$ for the **cardinality** of X .
- If C is a cardinality then we write 2^C for the cardinality of the powerset of a set of cardinality C .

Later on in Notation 2.26 we will write $a\#x$ for ‘ a is fresh for x ’. No connection is intended between $\#$ for cardinality and $\#$ for freshness, and it will always be clear what is meant.

Proposition 11.5 requires us to ensure a ‘generous’ supply of atoms. Notation 2.2 will help make this formal.

NOTATION 2.2. Given $l \leq \omega + 1$ define T_l by:

$$\mathsf{T}_0 = \#\mathbb{N} \quad \mathsf{T}_{l+1} = 2^{\mathsf{T}_l} \quad \mathsf{T}_\omega = \bigvee \{\mathsf{T}_l \mid l \in \omega\} \quad \mathsf{T}_{\omega+1} = 2^{\mathsf{T}_\omega}$$

It is easy to extend Notation 2.2, but $\mathsf{T}_{\omega+1}$ is as far as we will need to go in this paper.

REMARK 2.3. So for example, $\mathsf{T}_3 = 2^{\mathsf{T}_2} = 2^{2^{\mathsf{T}_1}} = 2^{2^{2^{\mathsf{T}_0}}} = 2^{2^{\#\mathbb{N}}}$.

We see that T_{l+1} has the cardinality of the powerset of (a set of cardinality) T_l and T_l has the same size as the l -fold powerset. In symbols,

$$\mathsf{T}_l = \#pset^l(\mathbb{N})$$

where by convention we take $pset^0(\mathbb{N})$ the 0-fold powerset of \mathbb{N} to be \mathbb{N} .

DEFINITION 2.4.— For each number $i \in \mathbb{Z}$ fix a disjoint set of **atoms** \mathbb{A}^i with $\#\mathbb{A}^i = \mathsf{T}_\omega$.

- Write $\mathbb{A} = \bigcup_{i \in \mathbb{Z}} \mathbb{A}^i$. Note by facts of cardinals that $\#\mathbb{A} = \mathsf{T}_\omega$.
- If $a \in \mathbb{A}$ (so a is an atom) write $level(a)$ for the unique number such that $a \in \mathbb{A}^{level(a)}$.
- We use a **permutative convention** that a, b, c, \dots range over *distinct* atoms.

If we do not wish to use the permutative convention then we will refer to the atom using n (see for instance $(\sigma \mathsf{eltatm})$ of Figure 1).

REMARK 2.5. We require $\#\mathbb{A} = \mathsf{T}_\omega$ so that we do not run out of atoms in the enumeration of Proposition 11.30 Search for uses of Proposition 11.5, and see also Subsection 10.6

Notation 2.6 will be useful shortly, we mention it now:

NOTATION 2.6. Suppose $A \subseteq \mathbb{A}$ and X is any set.³

- If $\#X < \aleph_\omega$ then call X **small**.
- If $A = \mathbb{A}^i \setminus A'$ for some $i \in \mathbb{Z}$ and some small $A' \subseteq \mathbb{A}^i$ then call A **cosmall** (in \mathbb{A}^i).
- If $\#X = \aleph_\omega$ then call X **generous**.

REMARK 2.7. ‘Small’ in this paper plays a similar role that ‘finite’ did in [Gab01; GP99; GP01].

The possibility of generalising beyond ‘finite’ in nominal techniques has been studied before [Che06; Gab07; Gab13; Gab12]. The basic character of nominal techniques changes little; the reader familiar with [GP01] can safely transfer their intuitions from that paper.

To see instances of how ‘small’ is used in this paper where finite could *not* be used, see Subsection 10.6 and Proposition 11.5.

The notion of ‘generous’ is new and can be related to ‘small’ as follows:

LEMMA 2.8. Suppose $i \in \mathbb{Z}$ and $A \subseteq \mathbb{A}^i$. Then A is generous if and only if A is not small.

If (anticipating Definition 2.34) we write $\forall a \in \mathbb{A}^i. \neg(a \in A)$ for ‘ A is small’ and $\exists a \in \mathbb{A}^i. a \in A$ for ‘ A is generous’ then we can write:

$$\exists a \in \mathbb{A}^i. a \in A \quad \Leftrightarrow \quad \neg \forall a \in \mathbb{A}^i. \neg(a \in A).$$

Proof. Clear from Definition 2.4. □

REMARK 2.9. So \exists is the dual to \forall —just as \exists is dual to \forall .

If the reader is versed in nominal techniques we note, making just for this paragraph entirely free use of nominal jargon, that \forall is self-dual—if A has small support, and small-supported generous sets are cosmall. However, we observe in Lemma 2.10(2) that there are generous sets that are not small-supported and are not cosmall. See also Remark 2.37.

LEMMA 2.10(1) If $A \subseteq \mathbb{A}^i$ is cosmall then it is generous.

(2) Not every generous $A \subseteq \mathbb{A}^i$ is cosmall.

Proof. Part 1 is from Lemma 2.8.

For part 2, we enumerate \mathbb{A}^i and consider a set of ‘every other element of \mathbb{A}^i ’

$$comb = \{a_0, a_2, a_4, \dots\}.$$

Clearly, $comb$ is generous but not cosmall. □

$comb$ is familiar and has helped us before, for instance in [DGM09, Definition 2] or [Gab11, Remark 2.18].

Lemma 2.11 is simple and will be useful. It lists the specific properties of smallness that we will need; they are also satisfied by finite sets:

LEMMA 2.11(1) A small union or intersection of finite sets is small.

(2) A finite union or intersection of cosmall sets is cosmall.

(3) Suppose $A \subseteq B \subseteq \mathbb{A}^i$ for $i \in \mathbb{Z}$. Then if B is small then so is A , and if A is cosmall then so is B .

(4) Suppose $A \subseteq B \subseteq \mathbb{A}^i$ for $i \in \mathbb{Z}$. Then if A is generous then so is B .

(5) If $A, B \subseteq \mathbb{A}^i$ and A is cosmall and B is generous, then $A \cap B$ is generous.

In particular, this will be useful: if A is cosmall and B is generous then $A \cap B$ is nonempty.

Proof. By elementary properties of sets and cardinalities. □

REMARK 2.12. We will use small and cosmall sets of atoms very shortly; generous sets of atoms will become useful later on, starting from Definition 8.3. To see Lemma 2.11(5) applied, see the important Lemma 8.14. See also Definition 2.34 and Remark 2.37.

³By ‘ X is any set’ we mean that it is just that: any collection of elements we like, that forms a set.

2.1.2. Permutation actions on sets

DEFINITION 2.13.— A **permutation** π is a bijection on atoms such that there exists some $j \in \mathbb{Z}$ such that for every $i \in \mathbb{Z}$, if $a \in \mathbb{A}^i$ then $\pi(a) \in \mathbb{A}^{i+j}$.

We call this constant j the **shift** of π , and we may write it $\text{shift}(\pi)$.

— If $\text{nontriv}(\pi) = \{a \mid \pi(a) \neq a\}$ is finite then we call π **finite**.

(Since \mathbb{A}^i is infinite for every $i \in \mathbb{Z}$, a finite π must necessarily satisfy $\text{shift}(\pi) = 0$.)

— If $\text{shift}(\pi) = 1$ then we call π a **shift-by-one permutation**, or just a **shift permutation**, when the size of the shift is evident.

LEMMA 2.14. *Shift(-by-one) permutations exist.*

Proof. By construction in Definition 2.4 we have $\#\mathbb{A}^i = \#\mathbb{A}^{i+1} = \top_\omega$ for every $i \in \mathbb{Z}$. Thus, the two sets can be bijected. \square

We will use the following notations in the rest of this paper:

NOTATION 2.15. Write id for the **identity** permutation such that $\text{id}(a) = a$ for all a . Write $\pi' \circ \pi$ for composition, so that $(\pi' \circ \pi)(a) = \pi'(\pi(a))$. If $i \in \mathbb{Z}$ and $a, b \in \mathbb{A}^i$ then write $(a \ b)$ for the **swapping** (terminology from [GP01]) mapping a to b , b to a , and all other c to themselves, and take $(a \ a) = \text{id}$.

NOTATION 2.16. Suppose π is a permutation and suppose $j \in \mathbb{Z}$.

Write π^{-1} for the inverse of π , so that $\pi^{-1} \circ \pi = \text{id} = \pi \circ \pi^{-1}$. Extend this to $\pi^j \cdot x$ as standard:

$$\begin{aligned} \pi^0 \cdot x &= x \\ \pi^{j-1} &= \pi^{-1} \cdot (\pi^j \cdot x) & \text{if } j < 0 \\ \pi^{j+1} &= \pi \cdot (\pi^j \cdot x) & \text{if } j > 0 \end{aligned}$$

So we can write $\pi^j = \overbrace{\pi \circ \dots \circ \pi}^{j \text{ times}}$.

NOTATION 2.17. Henceforth:

— π will range exclusively over *finite permutations* unless stated otherwise (we state otherwise just once: in Theorem 2.31).

— ϑ will always range over *shift permutations*.

— If we refer to ‘a permutation’ without further clarification then we mean a *finite* permutation.

Finite permutations π will interest us initially; later on in Section 8 we will also use shift permutations ϑ . These will always be called ϑ and will be explicitly described as *shift* permutations.

NOTATION 2.18. If $A \subseteq \mathbb{A}$ write

$$\text{fix}(A) = \{\pi \mid \forall a \in A. \pi(a) = a\}.$$

DEFINITION 2.19. A **set with a permutation action** X is a pair $(|X|, \cdot)$ of an **underlying set** $|X|$ and a **permutation action** written $\pi \cdot x$ which is a group action on $|X|$, so that $\text{id} \cdot x = x$ and $\pi \cdot (\pi' \cdot x) = (\pi \circ \pi') \cdot x$ for all $x \in X$ and permutations π and π' .

DEFINITION 2.20. Say that $A \subseteq \mathbb{A}$ **supports** $x \in X$ when $\forall \pi. \pi \in \text{fix}(A) \Rightarrow \pi \cdot x = x$. If a small $A \subseteq \mathbb{A}$ supporting x exists, call x **small-supported** (by A) and say that x has **small support**.

NOTATION 2.21. If X is a set with a permutation action then we may write

— $x \in X$ as shorthand for $x \in |X|$, and

— $X \subseteq X$ as shorthand for $X \subseteq |X|$.

We will only use Notation 2.22 for the case of a shift permutation, whence the use of ϑ :

NOTATION 2.22. Suppose X is a set with a permutation action and $x \in X$. Suppose ϑ is a shift permutation. Then:

— Call x **ϑ -ambiguous** when $\vartheta \cdot x = x$.

— Call x **ambiguous** when there exists a shift permutation ϑ such that x is ϑ -ambiguous.

2.1.3. Nominal sets.

DEFINITION 2.23. Call a set with a permutation action X a **nominal set** when every $x \in X$ has small support. X, Y, Z will range over nominal sets.

DEFINITION 2.24. Call a function $f \in X \Rightarrow Y$ **equivariant** when $\pi \cdot (f(x)) = f(\pi \cdot x)$ for all permutations π and $x \in X$. In this case write $f : X \Rightarrow Y$.

The category of nominal sets and equivariant functions between them is usually called the category of *nominal sets*.

DEFINITION 2.25. Suppose X is a nominal set and $x \in X$. Define the **support** of x by

$$\text{supp}(x) = \bigcap \{A \subseteq \mathbb{A} \mid A \text{ is small and supports } x\}.$$

NOTATION 2.26.— Write $a\#x$ as shorthand for $a \notin \text{supp}(x)$ and read this as a is **fresh for** x .

— If $T \subseteq \mathbb{A}$ write $T\#x$ as shorthand for $\forall a \in T. a\#x$.

— Given atoms a_1, \dots, a_n and elements x_1, \dots, x_m write $a_1, \dots, a_n\#x_1, \dots, x_m$ as shorthand for $\forall 1 \leq j \leq m. \{a_1, \dots, a_n\}\#x_j$. That is: $a_i\#x_j$ for every i and j .

THEOREM 2.27. Suppose X is a nominal set and $x \in X$. Then $\text{supp}(x)$ is the unique least small set of atoms that supports x .

Proof. Consider a permutation $\pi \in \text{fix}(\text{supp}(x))$. Write $\{a_1, \dots, a_n\} = \text{nontriv}(\pi)$ and choose any small $A \subseteq \mathbb{A}$ that supports x , so by construction $\text{supp}(x) \subseteq A$.

Let $\{b_1, \dots, b_n\}$ be a choice of fresh atoms; so $b_i \notin A \cup \{a_1, \dots, a_n\}$ for $1 \leq i \leq n$. Write $\tau = (b_1 a_1) \circ \dots \circ (b_n a_n)$. It is a fact that $(\tau \circ \pi \circ \tau)(a) = a$ for every $a \in A$ so $\tau \circ \pi \circ \tau \in \text{fix}(A)$. Also by the group action $(\tau \circ \pi \circ \tau) \cdot x = \tau \cdot (\pi \cdot (\tau \cdot x))$. Since A supports x , we have $\tau \cdot (\pi \cdot (\tau \cdot x)) = x$. We apply τ to both sides and note that $\tau \cdot x = x$, and it follows that $\pi \cdot x = x$. \square

COROLLARY 2.28(1) If $\pi(a) = a$ for all $a \in \text{supp}(x)$ then $\pi \cdot x = x$. Equivalently:

- (i) If $\pi \in \text{fix}(\text{supp}(x))$ then $\pi \cdot x = x$.
- (ii) If $\forall a \in \mathbb{A}. (\pi(a) \neq a \Rightarrow a\#x)$ then $\pi \cdot x = x$ (see Notation 2.26).
- (2) If $\pi(a) = \pi'(a)$ for every $a \in \text{supp}(x)$ then $\pi \cdot x = \pi' \cdot x$.
- (3) $a\#x$ if and only if $\exists b. (b\#x \wedge (b a) \cdot x = x)$.

Proof. By routine calculations from the definitions and from Theorem 2.27. \square

2.2. Examples

Suppose X and Y are nominal sets. We consider some examples, some of which will be useful later.

2.2.1. *Atoms.* \mathbb{A} is a nominal set with the *natural permutation action* $\pi \cdot a = \pi(a)$.

2.2.2. *Cartesian product.* $X \times Y$ is a nominal set with underlying set $\{(x, y) \mid x \in X, y \in Y\}$ and the *pointwise action* $\pi \cdot (x, y) = (\pi \cdot x, \pi \cdot y)$.

It is routine to check that $\text{supp}((x, y)) = \text{supp}(x) \cup \text{supp}(y)$.

2.2.3. *Full function space.* $X \rightarrow Y$ is a set with a permutation action with underlying set all functions from $|X|$ to $|Y|$, and the **conjugation** permutation action

$$(\pi \cdot f)(x) = \pi \cdot (f(\pi^{-1} \cdot x)).$$

2.2.4. *Small-supported function space.* $X \Rightarrow Y$ is a nominal set with underlying set the functions from $|X|$ to $|Y|$ with small support under the conjugation action, and the conjugation permutation action.

2.2.5. Full powerset

DEFINITION 2.29. Suppose Z is a set with a permutation action. Give subsets $Z \subseteq Z$ the **pointwise** permutation action

$$\pi \cdot Z = \{\pi \cdot z \mid z \in Z\}.$$

Then $pset(Z)$ (the full powerset of Z) is a set with a permutation action with

- underlying set $\{Z \mid Z \subseteq Z\}$ (the set of all subsets of $|Z|$), and
- the pointwise action $\pi \cdot Z = \{\pi \cdot z \mid z \in Z\}$.

A particularly useful instance of the pointwise action is for sets of atoms. As discussed in Subsection 2.2.1 above, if $a \in \mathbb{A}$ then $\pi \cdot a = \pi(a)$. Thus if $A \subseteq \mathbb{A}$ then

$$\pi \cdot A \quad \text{means} \quad \{\pi(a) \mid a \in A\}.$$

LEMMA 2.30. *Even if Z is a nominal set, $pset(Z)$ need not be a nominal set.*

Proof. Take Z to be equal to *comb* from the proof of Lemma 2.10. This does not have small support, though permutations still act on it pointwise. For more discussion see [Gab11, Remark 2.18]. \square

We consider further examples in Subsection 2.4.

2.3. The principle of equivariance and two nominal quantifiers

2.3.1. *Equivariance.* We come to Theorem 2.31, which is central to the ‘look and feel’ of nominal techniques. It enables a particularly efficient management of renaming and α -conversion in syntax and semantics and captures why it is so useful to use *names* in the foundations of our semantics and not, for instance, numbers.

Names are by definition symmetric (i.e. can be permuted). Taking names and permutations as *primitive* implies that permutations propagate to the things we build using them. This is the *principle of equivariance* (Theorem 2.31 below; see also [Gab11, Subsection 4.2] and [GP01, Lemma 4.7]).

The principle of equivariance implies that, provided we permute names uniformly in all the parameters of our definitions and theorems, we then get another valid set of definitions and theorems. This is not true of e.g. numbers, because numbers are equipped by construction with canonical properties such as *less than or equal to* \leq , which put them in order. By design, atoms do not have that.

THEOREM 2.31. *Suppose \bar{x} is a list x_1, \dots, x_n . Suppose π is a (not necessarily finite) permutation and write $\pi \cdot \bar{x}$ for $\pi \cdot x_1, \dots, \pi \cdot x_n$.*

Suppose $\Phi(\bar{x})$ is a first-order logic predicate with free variables \bar{x} . Suppose $\Upsilon(\bar{x})$ is a function specified using a first-order predicate with free variables \bar{x} . Suppose further that neither Φ nor Υ use only properties of indexes $i \in \mathbb{Z}$ that are invariant under translations, so that for instance the property ‘the index i of $a \in \mathbb{A}^i$ is even’ or ‘the index i of $a \in \mathbb{A}^i$ is a prime number’ are not allowed.⁴

Then we have the following principles:

- (1) **Equivariance of predicates.** $\Phi(\bar{x}) \Leftrightarrow \Phi(\pi \cdot \bar{x})$.⁵
- (2) **Equivariance of functions.** $\pi \cdot \Upsilon(\bar{x}) = \Upsilon(\pi \cdot \bar{x})$.
- (3) **Conservation of support.** *If \bar{x} denotes elements with small support then $\text{supp}(\Upsilon(\bar{x})) \subseteq \text{supp}(x_1) \cup \dots \cup \text{supp}(x_n)$.*

Proof. See Theorem 4.4, Corollary 4.6, and Theorem 4.7 from [Gab11]. \square

⁴Here we are paying our price for using *integers*, which are overly concrete, as an index for sets of atoms instead of a more abstract set with a group action outlined in Remark 9.29. This price seems worth paying for now, but we could hope to be more abstract in other, later papers.

⁵It is important to realise here that \bar{x} must contain *all* the variables mentioned in the predicate. It is not the case that $a = a$ if and only if $a = b$ —but it is the case that $a = b$ if and only if $b = a$ (both are false).

REMARK 2.32. Theorem 2.31 is three fancy ways of observing that if a specification is symmetric in atoms, then the result must be at least as symmetric as the inputs. We will use Theorem 2.31 frequently in this paper, either to move permutations around (parts 1 and 2) or to get ‘free’ bounds on the support of elements (part 3).

‘Free’ here means ‘we know it from the form of the definition, without having to verify it by concrete calculations’. Theorem 2.31, and also Theorem 2.39 below, are ‘free’ in the spirit of Wadler’s marvellously titled *Theorems for free!* [Wad89].

PROPOSITION 2.33. $\text{supp}(\pi \cdot x) = \pi \cdot \text{supp}(x)$ (which means $\{\pi(a) \mid a \in \text{supp}(x)\}$).

Using Notation 2.26, $a \# \pi \cdot x$ if and only if $\pi^{-1}(a) \# x$, and $a \# x$ if and only if $\pi(a) \# \pi \cdot x$.

Proof. Immediate consequence of part 2 of Theorem 2.31 (for the ‘not-free’ proof by concrete calculations see [Gab11, Theorem 2.19]). \square

2.3.2. *The New and the Generous quantifiers.* Recall from Notation 2.6 the notions of *cosmall* and *generous* sets of atoms:

DEFINITION 2.34. Suppose $i \in \mathbb{Z}$. We write:

$$\begin{array}{ll} \mathcal{I}a \in \mathbb{A}^i. \Phi(a) & \text{for } \{a \in \mathbb{A}^i \mid \Phi(a)\} \text{ is cosmall} \\ \mathcal{D}a \in \mathbb{A}^i. \Phi(a) & \text{for } \{a \in \mathbb{A}^i \mid \Phi(a)\} \text{ is generous} \end{array}$$

NOTATION 2.35. We may write $\mathcal{I}a_1 \dots a_n. \Phi(a_1, \dots, a_n)$ for $\mathcal{I}a_1 \dots \mathcal{I}a_n. \Phi(a_1, \dots, a_n)$.

REMARK 2.36 (The New quantifier). We call \mathcal{I} the **\mathcal{I} quantifier** (*New quantifier*). This is a ‘for most’ quantifier [Wes89], and is a *generalised quantifier* [KW96, Section 1.2.1].

We can read New as ‘for all but a small number $a \in \mathbb{A}^i$ ’, ‘for cosmall many a in \mathbb{A}^i ’, ‘for fresh a ’, or ‘for new a ’. It captures a *generative* aspect of names, that for any x we can find plenty of atoms a such that $a \notin \text{supp}(x)$. \mathcal{I} was designed in [GP01] to model the quantifier being used when we informally write “rename x in $\lambda x. t$ to be fresh”, or “emit a fresh channel name” or “generate a fresh memory cell”.

REMARK 2.37 (The Generous quantifier). The *Generous* quantifier \mathcal{D} is new⁶ in a nominal context. It is the dual to \mathcal{I} , that is: $\mathcal{D}a \in \mathbb{A}^i. \Phi(a) \Leftrightarrow \neg \mathcal{I}a \in \mathbb{A}^i. \neg \Phi(a)$, much as \exists is the dual to \forall .

$\mathcal{D}a. \Phi(a)$ ensures enough atoms satisfying Φ exist that no small set of atoms can exhaust our supply. $\mathcal{I}a. \Phi(a)$ also ensures this, but it also implies that no more than a small number of atoms satisfy $\neg \Phi(a)$, which may be too strong: in this paper, sometimes we will want to guarantee a plentiful supply of atoms with a certain property, but also allow a plentiful supply of atoms *without* that property. In other words, we do *not* want the sets intersection of two generous sets of atoms to be generous. For this, \mathcal{I} would be too strong and \mathcal{D} is what we need instead.

In symbols, \mathcal{D} is interesting because it is a quantifier satisfying the following two properties:

- (1) $\mathcal{D}a. \Phi(a) \wedge \mathcal{I}a. \Psi(a)$ implies $\mathcal{D}a. (\Phi(a) \wedge \Psi(a))$ and $\exists a. (\Phi(a) \wedge \Psi(a))$.
- (2) $\mathcal{D}a. \Phi(a) \wedge \mathcal{D}a. \Psi(a)$ does *not* imply $\mathcal{D}a. (\Phi(a) \wedge \Psi(a))$.

So on its own, Generous is just a *generalised quantifier* [Wes89; KW96]. There may seem nothing special about it. However, it is useful because of its good interaction with \mathcal{I} and \exists and weak interaction with sets intersection. See also Remark 2.41.

REMARK 2.38. We return to discuss \mathcal{I} . It is impossible to overstate the importance and convenience of the \mathcal{I} -quantifier and Theorem 2.39, below. \mathcal{I} over nominal sets satisfies the *some/any property* that

- to prove a \mathcal{I} -quantified property we test it for *one* fresh atom; but
- we may use a \mathcal{I} -quantified property for *any* fresh atom.

⁶No pun intended.

This \forall/\exists symmetry property is Theorem 2.39 and it arises *specifically* when \mathbb{I} is applied in a nominal context to symmetric atoms with an assumption of small support. We use it in this paper every time we write ‘Choose fresh a ’, without proving that it does not matter which fresh atom a we choose; it appears in the literature for instance as [Gab11, Theorem 6.5] and [GP01, Proposition 4.10].

THEOREM 2.39. *Suppose $\Phi(\bar{z}, a)$ is a predicate with free variables \bar{z}, a . Suppose \bar{z} denotes elements with small support. Then the following are equivalent:*

$$\forall a. (a \in \mathbb{A} \wedge a \# \bar{z}) \Rightarrow \Phi(\bar{z}, a) \quad \mathbb{I}a. \Phi(\bar{z}, a) \quad \exists a. a \in \mathbb{A} \wedge a \# \bar{z} \wedge \Phi(\bar{z}, a)$$

Proof. See Theorem 6.5 from [Gab11] or Proposition 4.10 from [GP01]. \square

Proof. Where convenient we may write \bar{z} as z_1, \dots, z_n .

— Suppose $\Phi(\bar{z}, a)$ holds for every atom $a \in \mathbb{A} \setminus \bigcup_{1 \leq i \leq n} \text{supp}(z_i)$.

By assumption \bar{z} denotes elements with small support, and it is a fact that a finite union of small sets is small, so $\mathbb{A} \setminus \bigcup_{1 \leq i \leq n} \text{supp}(z_i)$ is cosmall.

It follows that $\mathbb{I}a. \Phi(\bar{z}, a)$ holds.

— Suppose $A \subseteq \mathbb{A}$ is cosmall and $\Phi(\bar{z}, a)$ for every $a \in A$. As in the previous point, there exists some $a \in A$ such that $a \# z_i$ for every $1 \leq i \leq n$.

It follows that $\exists a \in \mathbb{A}. (a \# \bar{z} \wedge \Phi(\bar{z}, a))$.

— Now suppose $\Phi(\bar{z}, a)$ holds for some $a \in \mathbb{A} \setminus \bigcup_{1 \leq i \leq n} \text{supp}(z_i)$.

By Theorem 2.31(1) $\Phi((a' \cdot a) \cdot \bar{z}, a')$ holds for any $a' \in \mathbb{A}$. Choosing $a' \# \bar{z}$ we have by Corollary 2.28(1) that $(a' \cdot a) \cdot z_i = z_i$ for every $1 \leq i \leq n$.

Thus $\forall a \in \mathbb{A}. (a \# \bar{z} \Rightarrow \Phi(\bar{z}, a))$ holds. \square

REMARK 2.40. It is important to notice that Theorem 2.39 applies only if the ‘other variables’ \bar{z} denote elements with small support. If these elements do not have small support then Theorem 2.39 need not hold. The interested reader can see Lemma 2.61(3), which implicitly contains a counterexample.

We will be interested both in small-supported elements (e.g. internal predicates and sets, and their denotations) and non-small-supported elements (e.g. prepoints and points). See Definitions 3.1 and 5.4, and Definitions 5.3 and 8.3. To use the terminology of Definitions 2.19 and 2.23: we will need nominal sets and also sets with a permutation action.

REMARK 2.41. It is easy to see that we can translate Lemma 2.11(5) into quantifier notation as follows:

$$\begin{aligned} (\mathbb{I}a \in \mathbb{A}^i. \Phi(a) \wedge \exists a \in \mathbb{A}^i. \Psi(a)) &\Rightarrow \exists a \in \mathbb{A}^i. (\Phi \wedge \Psi) \\ (\mathbb{I}a \in \mathbb{A}^i. \Phi(a) \wedge \exists a \in \mathbb{A}^i. \Psi(a)) &\Rightarrow \exists a \in \mathbb{A}^i. (\Phi \wedge \Psi) \end{aligned}$$

In the text below we may write ‘cosmall’ and ‘generous’, or we may write \mathbb{I} and \exists , just depending on what seems most readable in each particular case. Either way, the underlying maths is the same.

2.4. Further examples

We now consider some slightly more technically challenging examples.

2.4.1. Small-supported powerset

DEFINITION 2.42. Suppose X is a set with a permutation action (it does not have to be a nominal set). Then let $\text{nomPset}(X)$ (the **small-supported powerset**) be the nominal set with

- underlying set those $X \subseteq X$ that are small-supported, and
- the **pointwise** action $\pi \cdot X = \{\pi \cdot x \mid x \in X\}$ inherited from Definition 2.29.

REMARK 2.43. If X is a nominal set then $\text{nomPset}(X)$ is the powerset object in the category of nominal sets [Gab11, Lemma 9.10]. However, we do not need X to be a nominal set in order that $\text{nomPset}(X)$ be a nominal set; we only need a permutation action on the elements and we can form the set of small-supported subsets.

DEFINITION 2.44. Suppose X is a set with a permutation action and $X \in \text{nomPset}(X)$. Call X **equivariant** when $\text{supp}(X) = \emptyset$; using Notation 2.26 we write $a\#X$ for every a .

Lemma 2.45 gives an alternative concrete characterisation of Definition 2.44; we will also return to this in Lemma 10.25:

LEMMA 2.45. *Suppose X is a set with a permutation action. Then*

$$X \subseteq X \text{ is equivariant} \quad \text{if and only if} \quad \forall x \in X. x \in X \Leftrightarrow \pi \cdot x \in X.$$

Lemma 2.46 notes a common misconception:⁷

LEMMA 2.46. *Suppose $X \subseteq X$ is small-supported and $x \in X$. Then:*

- (1) *It need not be the case that $\text{supp}(x) \subseteq \text{supp}(X)$.
Using Notation 2.26, we can write: $a\#X \subseteq X$ does not necessarily imply $a\#x \in X$.*
- (2) *Furthermore, it need not even be the case x has small support.*

Proof. (1) A counterexample is $X = X = \mathbb{A}$. It is a fact that $\text{supp}(X) = \emptyset$ and for any $a \in X$ we have $\text{supp}(a) = \{a\} \not\subseteq \emptyset$.

- (2) A counterexample is the full powerset X from Subsection 2.2.5. This has empty support, but it contains elements (such as *comb* from the proof of Lemma 2.10) without small support. \square

2.4.2. *Finite powerset.* For this subsection, fix a nominal set X .

DEFINITION 2.47. Write $\text{FinPow}(X)$ for the nominal set with

- underlying set the set of all finite subsets of X ,
- with the pointwise action from Definitions 2.29 and 2.42.

NOTATION 2.48. We might write $X \subseteq_{\text{fin}} X$ for $X \in \text{FinPow}(X)$.

LEMMA 2.49. *If $X \subseteq_{\text{fin}} X$ then:*

- (1) $\bigcup \{ \text{supp}(x) \mid x \in X \}$ is small (Notation 2.6).
- (2) $\bigcup \{ \text{supp}(x) \mid x \in X \} = \text{supp}(X)$.
- (3) $x \in X$ implies $\text{supp}(x) \subseteq \text{supp}(X)$ (contrast this with Lemma 2.46).
Rewriting this using Notation 2.26: if $a\#X$ and $x \in X$ then $a\#x$.

Proof. The first part is immediate since by assumption there is some finite $A \subseteq \mathbb{A}$ that bounds $\text{supp}(x)$ for all $x \in X$. The second part follows by an easy calculation using part 3 of Corollary 2.28; full details are in [Gab11, Theorem 2.29], of which Lemma 2.49 is a special case. Part 3 follows from the first and second parts. \square

2.4.3. *Strictly small-supported powerset.* For this subsection, fix a nominal set X .

DEFINITION 2.50. Call $X \subseteq X$ **strictly supported** by $A \subseteq \mathbb{A}$ when

$$\forall x \in X. \text{supp}(x) \subseteq A.$$

If there exists some small A which strictly supports X , then call X **strictly small-supported**.

Write $\text{strict}(X)$ for the set of strictly small-supported $X \subseteq X$. That is:

$$\text{strict}(X) = \{ X \subseteq X \mid \exists A \subseteq \mathbb{A}. A \text{ small} \wedge X \text{ strictly supported by } A \}$$

Lemma 2.51 clearly generalises Lemma 2.49. Indeed, if ‘small’ is taken equal to ‘finite’ (as was the case in [GP01]) then the results coincide:

LEMMA 2.51. *If $X \in \text{strict}(X)$ then:*

- (1) $\bigcup \{ \text{supp}(x) \mid x \in X \}$ is small.
- (2) $\bigcup \{ \text{supp}(x) \mid x \in X \} = \text{supp}(X)$.

⁷Understanding this is a significant step towards understanding what nominal support really is.

- (3) If $X \subseteq \mathbb{X}$ is strictly small-supported then it is small-supported.
- (4) $x \in X$ implies $\text{supp}(x) \subseteq \text{supp}(X)$ (contrast this with Lemma 2.46).
Rewriting this using Notation 2.26: if $a \# X$ and $x \in X$ then $a \# x$.
- (5) $\text{strict}(\mathbb{X})$ with the pointwise permutation action is a nominal set.

Proof. As for Lemma 2.49. □

EXAMPLE 2.52(1) $\mathbb{A} \subseteq \mathbb{A}$ is small supported by \emptyset but not strictly small-supported by \emptyset .

- (2) $\emptyset \subseteq \mathbb{A}$ (which is a small set) is strictly small-supported by \emptyset .

For the reader who does not like examples based on the empty set:

- (3) $\mathbb{A} \setminus \{a\}$ is supported by $\{a\}$, which is a small set, but not strictly small-supported.
- (4) $\{a\}$ is supported by $\{a\}$ and also strictly small-supported by $\{a\}$.

LEMMA 2.53. Suppose \mathbb{X} is a finitely supported nominal set, so that $\text{supp}(x) \subseteq_{\text{fin}} \mathbb{A}$ for every $x \in \mathbb{X}$.

Then if $X \subseteq \mathbb{X}$ is small then X is strictly small-supported by $\bigcup \{\text{supp}(x) \mid x \in X\}$.

Proof. By assumption every $x \in X$ has finite support, so by Lemma 2.11(1) the small union $\bigcup_{x \in X} \text{supp}(x)$ is small. It follows by an easy calculation using Theorem 2.31 that $\bigcup_{x \in X} \text{supp}(x)$ supports X . □

2.5. The NEW-quantifier for nominal sets

For this Subsection, suppose \mathbb{X} is a set with a permutation action.

DEFINITION 2.54. Suppose $X \subseteq \mathbb{X}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$.

Define the **new-quantifier on sets with a permutation action**—or just **new-quantifier on sets**—by

$$\mathbb{A}a.X = \{x \in \mathbb{X} \mid \mathbb{A}a' \in \mathbb{A}^i. (a' a) \cdot x \in X\}.$$

REMARK 2.55. $\mathbb{A}a.X$ was written $\mathbb{N}a.X$ in [GLP11, Definition 5.2], and goes back to [Gab09] where it was written $X - a$.

LEMMA 2.56. Suppose $x \in \mathbb{X}$ and $X \subseteq \mathbb{X}$ is small-supported. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$x \in \mathbb{A}a.X \Leftrightarrow \mathbb{A}a' \in \mathbb{A}^i. (a' a) \cdot x \in X.$$

Proof. Immediate from Definition 2.54. □

LEMMA 2.57. Suppose $X \subseteq \mathbb{X}$ is small-supported and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$\text{supp}(\mathbb{A}a.X) \subseteq \text{supp}(X) \setminus \{a\}.$$

Proof. By a routine calculation using Corollary 2.28. □

Recall from Subsection 2.4.1 the notion of small-supported powerset.

LEMMA 2.58. If $X \subseteq \mathbb{X}$ is small-supported then so is $\mathbb{A}a.X$.

Proof. This amounts to showing that if $X \subseteq \mathbb{X}$ has small support then so does $\mathbb{A}a.X \subseteq \mathbb{X}$. This follows by Lemma 2.57 or direct from Theorem 2.31. □

LEMMA 2.59. Suppose $X \subseteq \mathbb{X}$ is small-supported and suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$a \# X \text{ implies } X = \mathbb{A}a.X.$$

Proof. We reason as follows:

$$\begin{aligned} x \in \mathbb{A}a.X &\Leftrightarrow \mathbb{A}a' \in \mathbb{A}^i. (a' a) \cdot x \in X && \text{Definition 2.54} \\ &\Leftrightarrow \mathbb{A}a' \in \mathbb{A}^i. x \in (a' a) \cdot X && \text{Theorem 2.31} \\ &\Leftrightarrow \mathbb{A}a' \in \mathbb{A}^i. x \in X && \text{Corollary 2.28(1), } a', a \# X \\ &\Leftrightarrow x \in X && \text{Fact} \end{aligned}$$

□

LEMMA 2.60. Suppose $X, Y \subseteq \mathbb{X}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$X \subseteq Y \text{ implies } \mathcal{U}a.X \subseteq \mathcal{U}a.Y.$$

Proof. We reason as follows:

$$\begin{aligned} x \in \mathcal{U}a.X &\Leftrightarrow \mathcal{U}a' \in \mathbb{A}^i. (a' a) \cdot x \in X && \text{Definition 2.54} \\ &\Rightarrow \mathcal{U}a' \in \mathbb{A}^i. (a' a) \cdot x \in Y && X \subseteq Y \end{aligned}$$

□

LEMMA 2.61. Fix $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then:

(1) $\mathcal{U}a$ commutes with the intersection small-supported sets.

In symbols, for small-supported $X, Y \subseteq \mathbb{X}$ we have

$$\mathcal{U}a.(X \cap Y) = \mathcal{U}a.X \cap \mathcal{U}a.Y.$$

(2) If \mathbb{X} is a nominal set (so every $x \in \mathbb{X}$ has small support) then $\mathcal{U}a$ commutes with sets complement and union.

In symbols, for small-supported $X \subseteq \mathbb{X}$ we have

$$\mathcal{U}a.(\mathbb{X} \setminus X) = \mathbb{X} \setminus \mathcal{U}a.X \quad \text{and} \quad \mathcal{U}a.(X \cup Y) = \mathcal{U}a.X \cup \mathcal{U}a.Y.$$

(3) If \mathbb{X} is a set with a permutation action then $\mathcal{U}a$ does not necessarily commute with sets complement or union.

(4) If \mathbb{X} is a set with a permutation action and $X, Y \subseteq \mathbb{X}$ are small-supported and $a \# X$ then

$$\mathcal{U}a.(X \cup Y) = X \cup \mathcal{U}a.Y.$$

Proof. (1) We unpack Definition 2.54 and use Lemma 2.11(2).

(2) Suppose $(a' a) \cdot x \notin X$ for cosmall many $a' \in \mathbb{A}^i$. Then by sizes of sets of atoms, it is not the case that $(a' a) \cdot x \in X$ for cosmall many $a' \in \mathbb{A}^i$. Conversely suppose it is not the case that $(a' a) \cdot x \in X$ for cosmall many $a' \in \mathbb{A}^i$. By assumption x has small support, so there must exist some $a' \in \mathbb{A}^i$ such that $a' \# x$, X and $(a' a) \cdot x \notin X$. We use Theorem 2.39 (since x and X both have small support). The case of sets union is similar.

(3) Take $\mathbb{X} = \mathbb{A}^i$ and consider a comb set

$$\text{comb} = \{a_0, a_2, a_4, \dots\}$$

as used in the proof of Lemma 2.10.

It is easy to check that $\mathcal{U}a.\text{comb} = \emptyset$ and $\mathcal{U}a.(\mathbb{A}^i \setminus \text{comb}) = \emptyset$. Thus $\mathbb{A}^i \setminus \mathcal{U}a.\text{comb} \neq \mathcal{U}a.(\mathbb{A}^i \setminus \text{comb})$, and $\mathcal{U}a.(\text{comb} \cup (\mathbb{A}^i \setminus \text{comb})) \neq \mathcal{U}a.\text{comb} \cup (\mathcal{U}a.(\mathbb{A}^i \setminus \text{comb}))$.

(4) We reason as follows:

$$\begin{aligned} x \in \mathcal{U}a.(X \cup Y) &\Leftrightarrow \mathcal{U}a' \in \mathbb{A}^i. (a' a) \cdot x \in X \cup Y && \text{Definition 2.54} \\ &\Leftrightarrow \mathcal{U}a' \in \mathbb{A}^i. x \in (a' a) \cdot X \cup (a' a) \cdot Y && \text{Theorem 2.31} \\ &\Leftrightarrow \mathcal{U}a' \in \mathbb{A}^i. x \in X \cup (a' a) \cdot Y && \text{Corollary 2.28(1), } a, a' \# X \\ &\Leftrightarrow x \in X \vee \mathcal{U}a' \in \mathbb{A}^i. x \in (a' a) \cdot Y && \text{Fact} \\ &\Leftrightarrow x \in X \vee \mathcal{U}a' \in \mathbb{A}^i. (a' a) \cdot x \in X && \text{Theorem 2.31} \\ &\Leftrightarrow x \in X \cup \mathcal{U}a.Y && \text{Definition 2.54} \end{aligned}$$

□

2.6. Atoms-abstraction

Atoms-abstraction was the first real application of nominal techniques; it was used to build inductive datatypes of syntax-with-binding. In this paper we use it to model sets comprehension (see Definition 3.1). The maths here goes back to [Gab01; GP01]; we give references to proofs in a more recent presentation [Gab11].

Assume a nominal set \mathbb{X} and an $i \in \mathbb{Z}$.

DEFINITION 2.62. Let the **atoms-abstraction** set $[\mathbb{A}^i]\mathbb{X}$ have

- Underlying set $\{[a]x \mid a \in \mathbb{A}^i, x \in X\}$.
- Permutation action $\pi \cdot [a]x = [\pi \cdot a]\pi \cdot x$.

LEMMA 2.63. *If $x \in X$ and $a \in \mathbb{A}^i$ then $\text{supp}([a]x) = \text{supp}(x) \setminus \{a\}$. In particular $a \# [a]x$ (Notation 2.26).*

Proof. See [Gab11, Theorem 3.11]. □

LEMMA 2.64. *Suppose $x \in X$ and $a, b \in \mathbb{A}^i$. Then if $b \# x$ then $[a]x = [b](b \cdot a) \cdot x$.*

Proof. See [Gab11, Lemma 3.12]. □

LEMMA 2.65. *Suppose $b \in \mathbb{A}^i$ and $z \in [\mathbb{A}^i]X$. Then $b \# z$ implies $z @ b$ is well-defined and in X .*

Proof. See [Gab11, Theorem 3.19]. □

LEMMA 2.66. *Suppose $a \in \mathbb{A}^i$ and $x \in X$. Then:*

- (1) $([a]x) @ a = x$ and if $b \# x$ then $([a]x) @ b = (b \cdot a) \cdot x$.
- (2) If $a \# z$ then $[a](z @ a) = z$.

Proof. See [Gab11, Theorem 3.19]. □

Lemma 2.67 is a special case of [Gab11, Lemma 6.9] of [Gab01, Theorem 9.6.6]. It will often be useful:

LEMMA 2.67. *Suppose X and Y are nominal sets. Suppose $i \in \mathbb{Z}$ and $f : \mathbb{A}^i \times X \rightarrow Y$ is equivariant (Definition 2.24). Then*

$$\exists! y \in [\mathbb{A}^i]Y. \forall a \in \mathbb{A}^i. y = [a]f(a, x).$$

In words: there is a unique y in $[\mathbb{A}^i]Y$ which is equal to $f(a, x)$ for some/any fresh $a \in \mathbb{A}^i$.

Proof. Consider $a, a' \in \mathbb{A}^i$ fresh (so $a, a' \# x$). By Theorem 2.31 $a' \# [a]f(a, x)$. Therefore by Lemma 2.64 $[a]f(a, x) = [a'](a' \cdot a) \cdot f(a, x)$. By equivariance of f we have that $[a'](a' \cdot a) \cdot f(a, x) = [a']f(a', (a' \cdot a) \cdot x)$, so we are done. □

3. INTERNAL PREDICATES

3.1. Basic definition

DEFINITION 3.1. Define nominal abstract syntax datatypes **Pred** of **internal predicates** and **Setⁱ** for $i \in \mathbb{Z}$ of **internal (level i) sets** inductively as follows, where κ ranges over finite ordinals:

- $\text{Set}^i(0) = \{\text{atm}(a) \mid a \in \mathbb{A}^i\}$.
- If $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}(\kappa)$ then $\text{and}(\mathcal{X}) \in \text{Pred}(\kappa+1)$.
- If $X \in \text{Pred}(\kappa)$ then $\text{neg}(X) \in \text{Pred}(\kappa+1)$.
- If $X \in \text{Pred}(\kappa)$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ then $\text{all}[a]X \in \text{Pred}(\kappa+1)$.
- If $a \in \mathbb{A}^{i+1}$ and $x \in \text{Set}^i(\kappa)$ then $\text{elt}(x, a) \in \text{Pred}(\kappa+1)$.
- If $X \in \text{Pred}(\kappa)$ and $\kappa \leq \kappa'$ then $X \in \text{Pred}(\kappa')$.
- If $i \in \mathbb{Z}$ and $X \in \text{Pred}(\kappa)$ and $a \in \mathbb{A}^{i-1}$ then $[a]X \in \text{Set}^i(\kappa)$.
- If $x \in \text{Set}^i(\kappa)$ and $\kappa \leq \kappa'$ then $x \in \text{Set}^i(\kappa')$.

Define:

$$\text{Pred} = \bigcup_{\kappa} \text{Pred}(\kappa) \quad \text{Set}^i = \bigcup_{\kappa} \text{Set}^i(\kappa)$$

Write $\text{age}(X)$ for the least κ such that $X \in \text{Pred}_{\kappa}$ and $\text{age}(x)$ for the least κ such that $x \in \text{Set}^i(\kappa)$.

NOTATION 3.2.— If $a \in \mathbb{A}$ we may call $\text{atm}(a)$ an **internal atom**.

— If $X \in \text{Pred}$ we may call $[a]X$ an **internal comprehension**.

— We may call $\text{atm}(a)$ or $[a]X$ an **internal set**.⁸

REMARK 3.3. We read through and comment on Definition 3.1:

- κ measures the *age* or *stage* of an element; at what point in the induction it is introduced into the datatype. This is an inductive measure.
- If we elide κ and levels and simplify, we can rewrite Definition 3.1 semi-formally as follows:

$$\begin{aligned} x \in \text{Set} &::= \text{atm}(a) \mid [a]X \\ X \in \text{Pred} &::= \text{and}(\mathcal{X}) \mid \text{neg}(X) \mid \text{all}[a]X \mid \text{elt}(x, a) \end{aligned}$$

- and represents logical conjunction. neg represents negation. So if the reader sees $\text{neg}(X)$ they should mentally translate X to ‘ ϕ ’ and $\text{neg}(X)$ to ‘ $\neg\phi$ ’, and no harm will come of it.
- Truth \top is represented as $\text{and}(\emptyset)$. See Example 3.9.
- all represents universal quantification. In $\text{all}[a]X$, $[a]X$ is a nominal atoms-abstraction (Definition 2.62). It is used here to represent the binding of the universal quantifier; read $\text{all}[a]X$ as ‘for all a , X ’ or in symbols: ‘ $\forall a. \phi$ ’.
- elt represents a sets membership; read $\text{elt}(x, a)$ as ‘ x is an element of a ’. Note here that a is an atom; it does not literally have any elements. $\text{elt}(x, a)$ represents the predicate ‘we believe that x is an element of the variable a ’, or in symbols: ‘ $x \in a$ ’.
- $[a]X$ is used again to represent the binding of sets comprehension; read $[a]X$ as ‘the set of a such that ϕ ’ or in symbols: ‘ $\{a \mid \phi\}$ ’.⁹ If $a \in \mathbb{A}^i$ then $[a]X \in \text{Set}^{i+1}$.
- $\text{atm}(a)$ is a copy of $a \in \mathbb{A}$ wrapped in some formal syntax atm . We take $\text{atm}(a)$ as primitive in the syntax, but we want an extensional semantics so we should expect that some comprehension can be associated to it, if for the moment only intuitively. That intuition is $[b]\text{elt}(\text{atm}(b), a)$ or ‘ $\{b \mid b \in a\}$ ’. More on this in Remark 5.5.

REMARK 3.4. At first, we will be quite scrupulous about the distinction between a the atom and $\text{atm}(a)$ the internal set. Much later on in this paper, we may relax a little (if only for readability) and write ‘ a ’ where we should more properly write ‘ $\text{atm}(a)$ ’. For instance in Lemma 11.32 we write $\text{ext}^{\text{sq}} a = u$ and this means $\text{ext}^{\text{sq}} \text{atm}(a) = u$.

It will always be quite clear what is meant.

REMARK 3.5. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then we could write $\text{all}[a]X$ as $\text{all}(x)$, where $x \in \text{Set}^{i+1}$ is taken to be $[a]X$. In other words, we could view all as mapping Set^{i+1} to Pred , much as e.g. neg maps Pred to Pred or elt maps $\text{Set}^i \times \mathbb{A}^{i+1}$ to Pred .

This would be elegant, but less readable since we are used to a binder Q taking the syntactic form $Qa.T$. So we write $\text{all}[a]X$.

REMARK 3.6. Our syntax uses a nominal atoms-abstraction, which builds in α -equivalence properties in the standard way for nominal abstract syntax [GP01].

More advanced α -equivalence properties feature elsewhere: examples include Lemmas 2.57 and 4.7, the model of \forall over prepoints in Lemma 5.10, the carefully chosen use of nominal quantifiers in Definition 8.3, and Lemmas 10.26 and 10.27.

LEMMA 3.7. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$ and $a' \# X$. Then:

- (1) $[a]X = [a'](a' a) \cdot X$ and $\text{all}[a]X = \text{all}[a'](a' a) \cdot X$.
- (2) $a \# [a]X$ and $a \# \text{all}[a]X$, and $\text{supp}([a]X), \text{supp}(\text{all}[a]X) \subseteq \text{supp}(X) \setminus \{a\}$.

Proof. Immediate from Lemma 2.64, and Lemma 2.63 with Theorem 2.31. □

⁸So every internal comprehension or internal atom is an internal set. Another choice of terminology would be to call $\text{atm}(a)$ an internal atom, $[a]X$ an internal set, and $\text{atm}(a)$ or $[a]X$ *internal elements*.

However, note that $[a]X$ is not a set and neither is $\text{atm}(a)$; they are both syntax and we can call them what we like.

⁹We could wrap this in some extra formal syntax by writing $\text{comprehension}([a]X)$, but we do not bother.

3.2. Some useful notation

This subsection is organised as follows:

- Notation 3.8 aids readability.
- In Definition 3.11 we consider a simple example of an internal set.

Notation 3.8 will be useful later, but we mention it now as an example; the intended meaning of the notation should be clear:

NOTATION 3.8. Suppose $X, Y \in \text{Pred}$. Define syntactic sugar $\text{or}(X, Y)$, $\text{imp}(X, Y)$ and $\text{iff}(X, Y)$ by

$$\begin{aligned}\text{or}(X, Y) &= \text{neg}(\text{and}(\{\text{neg}(X), \text{neg}(Y)\})) \\ \text{imp}(X, Y) &= \text{or}(\{\text{neg}(X), Y\}) \\ \text{iff}(X, Y) &= \text{and}(\{\text{imp}(X, Y), \text{imp}(Y, X)\}).\end{aligned}$$

EXAMPLE 3.9. Define $\text{false} \in \text{Pred}$ and $\text{true} \in \text{Pred}$ by

$$\text{false} = \text{or}(\emptyset) \quad \text{and} \quad \text{true} = \text{and}(\emptyset).$$

Intuitively, false represents the empty disjunction, which is ‘internal false’, and true represents the empty conjunction, which is ‘internal truth’. We make this formal later, in Lemma 5.9(3).

For now we will be quite pedantic about notation, but later on we may relax this. From Notation 12.4 onwards we may write false as \perp and true as \top .

LEMMA 3.10. Suppose $i \in \mathbb{Z}$ and $a' \in \mathbb{A}^{i-1}$. Suppose $x \in \text{Set}^i$ and $a' \# x$. Then $x @ a' \in \text{Pred}$.

Proof. By Definition 3.1 $\text{Set}^i = [\mathbb{A}^{i-1}] \text{Pred}$. So this result just repeats Lemma 2.65. \square

Recall $\text{false} = \text{or}(\emptyset)$ from Example 3.9.

DEFINITION 3.11. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^{i-1}$. Define empt^i and set^i by

$$\begin{aligned}\text{empt}^i &= [a] \text{false} = [a] \text{or}(\emptyset) \\ \text{set}^i &= [a] \text{true} = [a] \text{and}(\emptyset).\end{aligned}$$

REMARK 3.12. Note that by Theorem 2.31 $a \# \text{false}$ and $a \# \text{true}$ for any $a \in \mathbb{A}^{i-1}$, and it follows by Lemma 2.67 that Definition 3.11 is well-defined (does not depend on the choice of a).

We conclude with an easy lemma:

LEMMA 3.13. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^{i-1}$. Then:

- (1) $\text{empt}^i @ a = \text{false}$ and $[a] \text{false} = \text{empt}^i$, and similarly $\text{set}^i @ a = \text{true}$ and $[a] \text{true} = \text{set}^i$.
- (2) $a \# \text{false}$ and $a \# \text{true}$.

Proof. (1) From Definition 3.11 and Lemma 2.66(1).

- (2) From part 1 of this result, since $a \# \text{false}$ by Theorem 2.31. \square

4. THE SIGMA-ACTION

4.1. Basic definitions and lemmas

Intuitively, Definition 4.1 defines a substitution action. It is slightly elaborate, especially because of (σelta) of Figure 1, so it gets a fancy name (‘ σ -action’) and we need to make formal and verify that it behaves as a substitution action should; see Remark 4.8.¹⁰

DEFINITION 4.1. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then define a σ -**action** (sigma-action) inductively by the rules in Figure 1. In that figure:

¹⁰There is more to the story, and to the name. The σ -action has a dual τ -action coming from nominal duality theory. More on this later, in Subsection 5.2. For now, if the reader mentally translates ‘ σ -action’ to ‘substitution action’, then their intuitions will most likely be correct.

(σand)		$\text{and}(\mathcal{X})[a \mapsto x] = \text{and}(\{X[a \mapsto x] \mid X \in \mathcal{X}\})$
(σneg)		$\text{neg}(X)[a \mapsto x] = \text{neg}(X[a \mapsto x])$
(σall)	$b \# x \Rightarrow$	$(\text{all}[b]X)[a \mapsto x] = \text{all}[b](X[a \mapsto x])$
(σeltatm)		$\text{elt}(y, a)[a \mapsto \text{atm}(n)] = \text{elt}(y[a \mapsto \text{atm}(n)], n)$
(σelta)		$\text{elt}(y, a)[a \mapsto [a']X] = X[a' \mapsto y[a \mapsto [a']X]]$
(σeltb)		$\text{elt}(y, b)[a \mapsto x] = \text{elt}(y[a \mapsto x], b)$
$(\sigma\mathbf{a})$		$\text{atm}(a)[a \mapsto x] = x$
$(\sigma\mathbf{b})$		$\text{atm}(b)[a \mapsto x] = \text{atm}(b)$
$(\sigma[])$	$c \# x \Rightarrow$	$([c]X)[a \mapsto x] = [c](X[a \mapsto x])$

Fig. 1: The sigma-action (Definition 4.1)

- In rule (σand) , $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}$.
- In rule (σneg) , $X \in \text{Pred}$.
- In rule (σall) , $X \in \text{Pred}$ and $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.
- In rule (σelta) , $a' \in \mathbb{A}^{i-1}$.
- In rule (σeltatm) , n ranges over *all* atoms in \mathbb{A}^i (not just those distinct from a).
- In rule (σeltb) , $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.
- In rule $(\sigma[])$, $X \in \text{Pred}$ and $c \in \mathbb{A}^k$ for some $k \in \mathbb{Z}$.

REMARK 4.2. Figure 1 slips in no fewer than three abuses of the mathematics:

- (1) We do not know that $X \in \text{Pred}$ implies $X[a \mapsto x] \in \text{Pred}$, so we should not write $\text{and}(\{X[a \mapsto x] \mid \dots\})$ on the right-hand side of (σand) , or indeed $X[a \mapsto x]$ on the right-hand side of (σneg) , and so on.
In fact, all right-hand sides of Figure 1 are suspect except those of $(\sigma\mathbf{a})$ and $(\sigma\mathbf{b})$.
- (2) We do not know whether the choice of fresh $a' \in \mathbb{A}^{i-1}$ in (σelta) matters, so we do not know that (σelta) is well-defined.
- (3) The definition looks inductive at first glance, however in the case of (σelta) there is no guarantee that X (on the right-hand side) is smaller than $\text{elt}(y, a)$ (on the left-hand side). The level of a' is strictly lower than the level of a , however levels are taken from \mathbb{Z} which is totally ordered but not well-ordered by \leq .

In fact:

- $X \in \text{Pred}$ does indeed imply $X[a \mapsto x] \in \text{Pred}$.
- The choice of fresh a' in (σelta) is immaterial.
- The levels of atoms involved are bounded below (see Definition 4.4) so we only ever work on a well-founded fragment of \mathbb{Z} .

For proofs see Proposition 4.6 and Lemma 4.7.

Would it be more rigorous to interleave the proofs of these lemmas with the definition, so that at each stage we are confident that what we are writing actually makes sense? Certainly we could; the reader inclined to worry about this need only read Definition 4.1 alongside Proposition 4.6 and Lemma 4.7 as a simultaneous inductive argument on $(\text{level}(a), \text{age}(X))$ lexicographically ordered.

REMARK 4.3 (Why ‘minimum level’). Levels are in \mathbb{Z} and are totally ordered by \leq but not well-founded (since integers can ‘go downwards forever’).

However, any (finite) internal predicate or internal set can mention only finitely many levels, so we can calculate the *minimum level* of a predicate or set, which is lower bound on the levels of atoms appearing in that predicate or set. We will use this lower bound to reason inductively on levels in Proposition 4.6 and Lemma 4.12.

DEFINITION 4.4. Define $\text{minlevel}(Z)$ and $\text{minlevel}(z)$ the **minimum level** of Z or z , inductively on $Z \in \text{Pred}$ and $z \in \text{Set}^i$ for $i \in \mathbb{Z}$ as follows:

$$\begin{aligned} \text{minlevel}(\text{atm}(a)) &= \text{level}(a) \\ \text{minlevel}(\text{and}(\mathcal{X})) &= \min(\{0\} \cup \{\text{minlevel}(X) \mid X \in \mathcal{X}\}) \\ \text{minlevel}(\text{neg}(X)) &= \text{minlevel}(X) \\ \text{minlevel}(\text{all}[a]X) &= \min(\{\text{level}(a), \text{minlevel}(X)\}) \\ \text{minlevel}(\text{elt}(x, a)) &= \min(\{\text{minlevel}(x), \text{level}(a)\}) \\ \text{minlevel}([a]X) &= \min(\{\text{level}(a), \text{minlevel}(X)\}) \end{aligned}$$

Above, $\min(\mathcal{I})$ is the least element of $\mathcal{I} \subseteq_{\text{fin}} \mathbb{Z}$. We add 0 in the clause for **and** as a ‘default value’ to exclude calculating a minimum for the empty set; any other fixed integer element would do as well or, if we do not want to make this choice, we can index minlevel over a fixed but arbitrary choice. The proofs to follow will not care.

It will be convenient to apply minlevel to a mixed list of internal predicates, atoms, and internal sets:

NOTATION 4.5.— Define $\text{minlevel}(a) = \text{level}(a)$.

— If $l = (l_1, l_2, \dots, l_n)$ is a list of elements from $\text{Pred} \cup \bigcup_{i \in \mathbb{Z}} \text{Set}^i \cup \mathbb{A}$ then we write $\text{minlevel}(l)$ for the least element of $\{\text{minlevel}(l_1), \dots, \text{minlevel}(l_n)\}$.

PROPOSITION 4.6. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$.

- (1) If $Z \in \text{Pred}$ then $Z[a \mapsto x]$ is well-defined, $\text{minlevel}(Z[a \mapsto x]) \geq \text{minlevel}(Z, a, x)$, and $Z[a \mapsto x] \in \text{Pred}$.
- (2) If $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ then $z[a \mapsto x]$ is well-defined, $\text{minlevel}(z[a \mapsto x]) \geq \text{minlevel}(z, a, x)$, and $z[a \mapsto x] \in \text{Set}^k$.

Proof. Fix some $k \in \mathbb{Z}$. We prove the Proposition for all Z, a, x and z, a, x such that $\text{minlevel}(Z, a, x) \geq k$ and $\text{minlevel}(z, a, x) \geq k$, by induction on $(\text{level}(a), \text{age}(Z))$ and $(\text{level}(a), \text{age}(z))$ lexicographically ordered. Since k was arbitrary, this suffices to prove it for all Z, a, x and z, a, x .

We consider the possibilities for $Z \in \text{Pred}$:

— *The case of $\text{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}$.*

By Figure 1 (σand) $Z[a \mapsto x] = \text{and}(\{X'[a \mapsto x] \mid X' \in \mathcal{X}\})$. We use the inductive hypothesis on each $X'[a \mapsto x]$ and some easy arithmetic calculations.

— *The case of $\text{neg}(X')$ for $X' \in \text{Pred}$.*

By Figure 1 (σneg) $Z[a \mapsto x] = \text{neg}(X'[a \mapsto x])$. We use the inductive hypothesis on $X'[a \mapsto x]$.

— *The case of $\text{all}[b]X'$ for $X' \in \text{Pred}$ and $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.*

Using Lemma 3.7(1) we may assume without loss of generality that $b \# x$. By Figure 1 (σall) $(\text{all}[b]X')[a \mapsto x] = \text{all}[b'](X[a \mapsto x])$. We use the inductive hypothesis on $X'[a \mapsto x]$.

— *The case of $\text{elt}(z, a)$ for $z \in \text{Set}^{i-1}$.* There are two sub-cases:

— *Suppose $x = \text{atm}(n)$ for some $n \in \mathbb{A}^i$.* By Figure 1 (σeltatm) $\text{elt}(z, a)[a \mapsto x] = \text{elt}(z[a \mapsto \text{atm}(n)], n)$. We use the inductive hypothesis on $z[a \mapsto \text{atm}(n)]$.

— *Suppose $x = [a'](x @ a')$ for some fresh $a' \in \mathbb{A}^{i-1}$ (so $a' \# x, z$).* By Figure 1 (σelta) $\text{elt}(z, a)[a \mapsto x] = (x @ a')[a' \mapsto z[a \mapsto x]]$. We have the inductive hypothesis on $z[a \mapsto x]$. We chose $a' \# x$ so by Lemma 3.10 $x @ a' \in \text{Pred}$. We also have the inductive hypothesis (since $k \leq \text{level}(a') = i-1 \leq i = \text{level}(a)$) on $(x @ a')[a' \mapsto z[a \mapsto x]]$, and this suffices.

— *The case of $\text{elt}(z, c)$ where $c \in \mathbb{A}^k$ and $z \in \text{Set}^{k-1}$ and $k \in \mathbb{Z}$.*

By Figure 1 (σeltb) and the inductive hypothesis.

We consider the possibilities for $z \in \text{Set}^k$:

— *The case that z is an internal atom.*

We use $(\sigma\mathbf{a})$ or $(\sigma\mathbf{b})$ of Figure 1.

— *The case that z is an internal comprehension.*

Choose fresh $c \in \mathbb{A}^{k-1}$ (so $c \# x, z$), so that by Lemma 2.66(2) $z = [c](z@c)$. We use the first part of this result and Figure 1 $(\sigma[])$. \square

4.2. Alpha-equivalence and substitution on \mathbf{elt}

LEMMA 4.7 $((\sigma\alpha))$. Suppose $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$ and $x \in \mathbf{Set}^i$. Suppose $Z \in \mathbf{Pred}$ and $a' \# Z$ and $k \in \mathbb{Z}$ and $z \in \mathbf{Set}^k$ and $a' \# z$. Then:

- (1) $Z[a \mapsto x] = ((a' a) \cdot Z)[a' \mapsto x]$ and $z[a \mapsto x] = ((a' a) \cdot z)[a' \mapsto x]$.
- (2) $\mathit{supp}(Z[a \mapsto x]) \subseteq (\mathit{supp}(Z) \setminus \{a\}) \cup \mathit{supp}(x)$ and $\mathit{supp}(z[a \mapsto x]) \subseteq (\mathit{supp}(z) \setminus \{a\}) \cup \mathit{supp}(x)$.
- (3) If $a \# x$ then $a \# Z[a \mapsto x]$ and $a \# z[a \mapsto x]$.

Proof. By induction on Z and z . We consider the possibilities for $Z \in \mathbf{Pred}$:

- *The case of $\mathbf{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{\text{fin}} \mathbf{Pred}$.* By Lemma 2.49 $a \# X'$ for every $X' \in \mathcal{X}$, so by the inductive hypothesis $X'[a \mapsto x] = ((a' a) \cdot X')[a' \mapsto x]$. We use Figure 1 $(\sigma\mathbf{int})$ and Theorem 2.31.
- *The case of $\mathbf{neg}(X)$ for $X \in \mathbf{Pred}$.* By Figure 1 $(\sigma\mathbf{neg})$ and the inductive hypothesis for X .
- *The case of $\mathbf{all}[b]X$ for $X \in \mathbf{Pred}$ and $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.* Using Lemma 3.7(1) we may assume without loss of generality that $b \# x$. We use Figure 1 $(\sigma\mathbf{all})$ and the inductive hypothesis.
- *The case of $\mathbf{elt}(y, a)$ for some $y \in \mathbf{Set}^{i-1}$.* There are two sub-cases:
 - Suppose $x = \mathbf{atm}(n)$ for some $n \in \mathbb{A}^k$. We reason as follows:

$$\begin{aligned} \mathbf{elt}(y, a)[a \mapsto \mathbf{atm}(n)] &= \mathbf{elt}(y[a \mapsto \mathbf{atm}(n)], n) && \text{Figure 1}(\sigma\mathbf{eltatm}) \\ &= \mathbf{elt}(((a' a) \cdot y)[a' \mapsto \mathbf{atm}(n)], n) && \text{Ind hyp for } y \\ &= \mathbf{elt}(((a' a) \cdot y), a')[a' \mapsto \mathbf{atm}(n)] && \text{Figure 1}(\sigma\mathbf{eltatm}) \\ &= ((a' a) \cdot \mathbf{elt}(y, a'))[a' \mapsto \mathbf{atm}(n)] && \text{Theorem 2.31} \end{aligned}$$

- Suppose $x = [b'](x@b')$ for some fresh $b' \in \mathbb{A}^{i-1}$ (so $b' \# x, y, z$ and $k \leq \text{level}(b')$). We reason as follows:

$$\begin{aligned} \mathbf{elt}(y, a)[a \mapsto x] &= (x@b')[b' \mapsto y[a \mapsto x]] && \text{Figure 1}(\sigma\mathbf{elta}) \\ &= (x@b')[b' \mapsto ((a' a) \cdot y)[a' \mapsto x]] && \text{Ind hyp for } y \\ &= \mathbf{elt}(((a' a) \cdot y), a')[a' \mapsto x] && \text{Figure 1}(\sigma\mathbf{elta}) \end{aligned}$$

- *The case $\mathbf{elt}(y, b)$ for $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $y \in \mathbf{Set}^{j-1}$.* We reason as follows:

$$\begin{aligned} \mathbf{elt}(y, b)[a \mapsto x] &= \mathbf{elt}(y[a \mapsto x], b) && \text{Figure 1}(\sigma\mathbf{eltb}) \\ &= \mathbf{elt}(((a' a) \cdot y)[a' \mapsto x], b) && \text{Ind hyp for } y \\ &= \mathbf{elt}(((a' a) \cdot y), b)[a' \mapsto x] && \text{Figure 1}(\sigma\mathbf{eltb}) \\ &= ((a' a) \cdot \mathbf{elt}(y, b))[a' \mapsto x] && \text{Theorem 2.31} \end{aligned}$$

We consider the possibilities for $z \in \mathbf{Set}^k$:

- *The case that z is an internal atom.* We use $(\sigma\mathbf{a})$ or $(\sigma\mathbf{b})$ of Figure 1.
- *The case that z is an internal comprehension.* We use Lemma 2.66(2) for a fresh $c \in \mathbb{A}^{k-1}$ (so $c \# z$), $(\sigma[])$, and the inductive hypothesis on $z@c$.

For part 2, we note that by Theorem 2.31 and Proposition 2.33

$$\begin{aligned} \mathit{supp}(Z[a \mapsto x]) &\subseteq \mathit{supp}(Z) \cup \{a\} \cup \mathit{supp}(x) \quad \text{and} \\ \mathit{supp}(((a' a) \cdot Z)[a' \mapsto x]) &\subseteq (a' a) \cdot \mathit{supp}(Z) \cup \{a'\} \cup \mathit{supp}(x). \end{aligned}$$

We take a sets intersection. The case of z is similar.

Part 3 follows, recalling from Notation 2.26 that $a \# x$ means $a \notin \mathit{supp}(x)$. \square

$(\sigma\alpha)$	$b' \# Z \Rightarrow$	$Z[b \mapsto y] = ((b' \ b) \cdot Z)[b' \mapsto y]$
$(\sigma\#)$	$b \# Z \Rightarrow$	$Z[b \mapsto y] = Z$
$(\sigma\sigma)$	$a \# y \Rightarrow$	$Z[a \mapsto x][b \mapsto y] = Z[b \mapsto y][a \mapsto x[b \mapsto y]]$
(σswp)	$a \# y, b \# x \Rightarrow$	$Z[a \mapsto x][b \mapsto y] = Z[b \mapsto y][a \mapsto x]$
(σasc)	$a \# y, b \# Z \Rightarrow$	$Z[a \mapsto x][b \mapsto y] = Z[a \mapsto x][b \mapsto y]$
(σid)		$Z[a \mapsto \text{atm}(a)] = Z$
(σren)	$a' \# Z \Rightarrow$	$Z[a \mapsto \text{atm}(a')] = (a' \ a) \cdot Z$
$(\sigma@)$	$c \# x \Rightarrow$	$(z@c)[a \mapsto x] = z[a \mapsto x]@c$

Fig. 2: Further nominal algebra properties of the σ -action

4.3. Further nominal algebra properties of the σ -action

REMARK 4.8. Many useful properties of the σ -action are naturally expressed as nominal algebra judgements—equalities subject to freshness conditions [GM09]. Some are listed for the reader’s convenience in Figure 2, which goes back to nominal axiomatic studies of substitution from [GM06; GM08].

In this paper we are dealing with a concrete model, so the judgements in Figure 2 not assumed and are not axioms. Instead they proved; they are propositions and lemmas:

- We saw $(\sigma\alpha)$ in Proposition 4.6.
- $(\sigma\#)$ is Lemma 4.9.
- $(\sigma\sigma)$ is Lemma 4.12.
- (σswp) and (σasc) are Corollaries 4.14 and 4.15.
- (σid) is Lemma 4.16.
- (σren) is Lemma 4.17.
- $(\sigma@)$ is Lemma 4.11.

These are familiar properties of substitution on syntax: for instance $(\sigma\alpha)$ looks like an α -equivalence property—and indeed that is exactly what it is—and $(\sigma\#)$ (Lemma 4.9) is sometimes called *garbage collection* and corresponds to the property “if a is not free in t then $t[a \mapsto s] = t$ ”.

This is expected: a feature of nominal techniques is that properties familiar from syntax reappear in some semantic form (e.g. ‘fresh for’ reflects ‘not free in’, or $(\sigma\#)$ reflects a familiar garbage-collection property).

But, the proofs of these properties are not replays of the familiar syntactic properties. Partly this because the proofs use (unfamiliar?) nominal reasoning, but also it is because the σ -action on Pred is not a simple ‘tree-grafting’—not even a capture-avoiding one—because of (σelta) in Figure 1. The proofs work, but we cannot take that for granted and they require checking.

4.3.1. Property $(\sigma\#)$ (garbage collection)

LEMMA 4.9 $(\sigma\#)$. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and $Z \in \text{Pred}$ and $z \in \text{Set}^k$ for $k \in \mathbb{Z}$. Then

$$\begin{aligned} a \# Z &\Rightarrow Z[a \mapsto x] = Z \\ a \# z &\Rightarrow z[a \mapsto x] = z. \end{aligned}$$

Proof. By induction on Z and z . We consider the possibilities for $Z \in \text{Pred}$:

- *The case of $\text{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}$.*
By Figure 1 (σand) $\text{and}(\mathcal{X})[a \mapsto x] = \text{and}(\{X[a \mapsto x] \mid X \in \mathcal{X}\})$. By Lemma 2.49(3) $a \# X$ for every $X \in \mathcal{X}$. We use the inductive hypothesis on each X .
- *The case of $\text{neg}(X)$ for $X \in \text{Pred}$.*
By Figure 1 (σneg) $\text{neg}(X)[a \mapsto x] = \text{neg}(X[a \mapsto x])$. We use the inductive hypothesis on X .
- *The case of $\text{all}[b]X$ for $X \in \text{Pred}$ and $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.*

Using Lemma 3.7(1) we may assume without loss of generality that $b\#x$. By Figure 1 (σall) $(\text{all}[b]X)[a\mapsto x] = \text{all}[b](X[a\mapsto x])$. We use the inductive hypothesis on X .

— *The case of $\text{elt}(y, a)$ for $i \in \mathbb{Z}$ and $y \in \text{Set}^{i-1}$.*

This is impossible because we assumed $a\#Z$.

— *The case of $\text{elt}(y, b)$ for $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $y \in \text{Set}^{j-1}$.*

By Figure 1 (σeltb) $\text{elt}(y, b)[a\mapsto x] = \text{elt}(y[a\mapsto x], b)$. We use the inductive hypothesis on y .

We consider the possibilities for $z \in \text{Set}^k$:

— If z is an internal atom then we reason using $(\sigma\mathbf{a})$ or $(\sigma\mathbf{b})$ of Figure 1.

— If z is an internal comprehension then we use Lemma 2.66(2) for a fresh $c \in \mathbb{A}^{k-1}$ (so $c\#z$), $(\sigma[])$, and the inductive hypothesis on $z@c$. \square

Recall $\text{false} = \text{or}(\emptyset)$ and $\text{true} = \text{and}(\emptyset)$ from Example 3.9. Corollary 4.10 is an easy consequence of Lemma 4.9 and will be useful later:

COROLLARY 4.10. *Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then*

$$\text{false}[a\mapsto x] = \text{false} \quad \text{and} \quad \text{true}[a\mapsto x] = \text{true}.$$

Proof. By Theorem 2.31 $\text{supp}(\text{false}) = \emptyset$ so that $a\#x$. We use Lemma 4.9. Similarly for true . \square

4.3.2. σ commutes with atoms-concretion. Lemma 4.11 will be useful later, starting with Lemma 4.12:

LEMMA 4.11 ($(\sigma@)$). *Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Suppose $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ and $c \in \mathbb{A}^{k-1}$ and $c\#z, x$. Then*

$$(z@c)[a\mapsto x] = z[a\mapsto x]@c.$$

Proof. Note that by Lemma 2.65 (since $c\#z$) $z@c$ exists. We reason as follows:

$$\begin{aligned} (z@c)[a\mapsto x] &= ([c]((z@c)[a\mapsto x]))@c && \text{Lemma 2.66(1)} \\ &= ([c](z@c))[a\mapsto x]@c && \text{Figure 1}(\sigma[]), c\#x \\ &= z[a\mapsto x]@c && \text{Lemma 2.66(2), } c\#z \end{aligned} \quad \square$$

4.3.3. σ commutes with itself: the ‘substitution lemma’. The inductive quantity we use in Lemma 4.12 will be $(\text{level}(a), \text{age}(Z))$, lexicographically ordered. It will become clear in the proof how this works:

LEMMA 4.12. *Suppose $Z \in \text{Pred}$ and $k \in \mathbb{Z}$ and $z \in \text{Set}^k$. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and suppose $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $y \in \text{Set}^j$ and $a\#y$. Then*

$$\begin{aligned} Z[a\mapsto x][b\mapsto y] &= Z[b\mapsto y][a\mapsto x[b\mapsto y]] \\ z[a\mapsto x][b\mapsto y] &= z[b\mapsto y][a\mapsto x[b\mapsto y]]. \end{aligned}$$

Proof. For brevity we may use syntactic sugar

$$\sigma \text{ for } [a\mapsto x][b\mapsto y] \quad \text{and} \quad \sigma' \text{ for } [b\mapsto y][a\mapsto x[b\mapsto y]].$$

Fix some $k \in \mathbb{Z}$. We prove the Lemma for all Z, a, x, b, y and z, a, x, b, y such that $\text{minlevel}(Z, a, x, b, y) \geq k$ and $\text{minlevel}(z, a, x, b, y) \geq k$ (Definition 4.4), reasoning by induction on $(\text{level}(a) + \text{level}(b), \text{age}(Z))$ and $(\text{level}(a) + \text{level}(b), \text{age}(z))$ lexicographically ordered. Since k was arbitrary, this suffices to prove it for all Z, a, x, b, y and z, a, x, b, y .

We consider the possibilities for $Z \in \text{Pred}$:

— *The case of $\text{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}$.* We use rule (σand) of Figure 1 and the inductive hypothesis.

— *The case of $\text{neg}(X)$ for $X \in \text{Pred}$.* We use (σneg) of Figure 1 and the inductive hypothesis.

- The case of $\text{all}[a']X$ for $X \in \text{Pred}$ and $a' \in \mathbb{A}^{i'}$ for some $i' \in \mathbb{Z}$. We use Lemma 3.7(1) to assume without loss of generality that $a' \# x, y$, and then we use (σall) of Figure 1 and the inductive hypothesis.
- The case of $\text{elt}(z, b)$ for $z \in \text{Set}^{j-1}$ where $j \in \mathbb{Z}$. There are two sub-cases:
 - Suppose $y = \text{atm}(n)$ for some $n \in \mathbb{A}^i$ other than a (we assumed $a \# y$ so $n = a$ is impossible). We reason as follows:

$$\begin{aligned}
 \text{elt}(z, b) [a \mapsto x] [b \mapsto \text{atm}(n)] & \\
 = \text{elt}(z [a \mapsto x], b) [b \mapsto \text{atm}(n)] & \quad \text{Figure 1}(\sigma \text{eltb}) \\
 = \text{elt}(z \sigma, n) & \quad \text{Figure 1}(\sigma \text{eltatm}) \\
 = \text{elt}(z \sigma', n) & \quad \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, b)), a \# y \\
 = \text{elt}(z [b \mapsto \text{atm}(n)], n) [a \mapsto x [b \mapsto \text{atm}(n)]] & \quad \text{Figure 1}(\sigma \text{eltb}) \\
 = \text{elt}(z, b) [b \mapsto \text{atm}(n)] [a \mapsto x [b \mapsto \text{atm}(n)]] & \quad \text{Figure 1}(\sigma \text{eltatm})
 \end{aligned}$$

- Suppose $y = [b'](y @ b')$ for some fresh $b' \in \mathbb{A}^{j-1}$ (so $b' \# z, x, y$ and $k \leq \text{level}(b')$). Note by Theorem 2.31 that $a \# y @ b'$ and $b' \# x [b \mapsto y]$. We reason as follows:

$$\begin{aligned}
 \text{elt}(z, b) [a \mapsto x] [b \mapsto y] & \\
 = \text{elt}(z [a \mapsto x], b) [b \mapsto y] & \quad \text{Figure 1}(\sigma \text{eltb}) \\
 = (y @ b') [b' \mapsto z \sigma] & \quad \text{Figure 1}(\sigma \text{elta}) \\
 = (y @ b') [b' \mapsto z \sigma'] & \quad \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, b)), a \# y \\
 = (y @ b') [a \mapsto x [b \mapsto y]] [b' \mapsto z \sigma'] & \quad \text{Lemma 4.9, } a \# y @ b' \\
 = (y @ b') [b' \mapsto z [b \mapsto y]] [a \mapsto x [b \mapsto y]] & \quad \text{IH } \text{level}(b') < \text{level}(b), b' \# x [b \mapsto y] \\
 = \text{elt}(z, b) [b \mapsto y] [a \mapsto x [b \mapsto y]] & \quad \text{Figure 1}(\sigma \text{elta})
 \end{aligned}$$

- The case of $\text{elt}(z, a)$ for $z \in \text{Set}^{i-1}$ where $i \in \mathbb{Z}$. There are two sub-cases:
 - Suppose $x = \text{atm}(n)$ for some $n \in \mathbb{A}^i$. If $n \neq b$ then we reason as follows:

$$\begin{aligned}
 \text{elt}(z, a) [a \mapsto \text{atm}(n)] [b \mapsto y] & \\
 = \text{elt}(z [a \mapsto \text{atm}(n)], n) [b \mapsto y] & \quad \text{Figure 1}(\sigma \text{eltatm}) \\
 = \text{elt}(z \sigma, n) & \quad \text{Figure 1}(\sigma \text{eltb}) \\
 = \text{elt}(z \sigma', n) & \quad \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, a)), a \# y \\
 = \text{elt}(z [b \mapsto y] [a \mapsto \text{atm}(n)], n) & \quad (\sigma \mathbf{b}) n \neq b \\
 = \text{elt}(z [b \mapsto y], a) [a \mapsto \text{atm}(n)] & \quad \text{Figure 1}(\sigma \text{eltatm}) \\
 = \text{elt}(z [b \mapsto y], a) [a \mapsto \text{atm}(n)] [b \mapsto y] & \quad (\sigma \mathbf{b}) n \neq b \\
 = \text{elt}(z, a) [b \mapsto y] [a \mapsto \text{atm}(n)] [b \mapsto y] & \quad \text{Figure 1}(\sigma \text{eltb})
 \end{aligned}$$

If $n = b$ so that $x = \text{atm}(b)$, and $y = \text{atm}(m)$ for some $m \in \mathbb{A}^j$ other than a , then we reason as follows:

$$\begin{aligned}
 \text{elt}(z, a) [a \mapsto \text{atm}(b)] [b \mapsto \text{atm}(m)] & \\
 = \text{elt}(z [a \mapsto \text{atm}(b)], b) [b \mapsto \text{atm}(m)] & \quad \text{Figure 1}(\sigma \text{eltatm}) \\
 = \text{elt}(z [a \mapsto \text{atm}(b)] [b \mapsto \text{atm}(m)], m) & \quad \text{Figure 1}(\sigma \text{eltatm}) \\
 = \text{elt}(z [b \mapsto \text{atm}(m)] [a \mapsto \text{atm}(b)] [b \mapsto \text{atm}(m)], m) & \quad \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, a)), a \# m \\
 = \text{elt}(z [b \mapsto \text{atm}(m)], m) [a \mapsto \text{atm}(b)] [b \mapsto \text{atm}(m)] & \quad \text{Figure 1}(\sigma \text{eltb}) \\
 = \text{elt}(z, b) [b \mapsto \text{atm}(m)] [a \mapsto \text{atm}(b)] [b \mapsto \text{atm}(m)] & \quad \text{Figure 1}(\sigma \text{eltatm})
 \end{aligned}$$

If $n=b$ so that $x=\text{atm}(b)$, and $y=[b'](y@b')$ for some fresh $b' \in \mathbb{A}^{j-1}$ (so $b' \# z, n, y$ and $k \leq \text{level}(b')$) then we reason as follows (note by Theorem 2.31 that $a \# y@b'$ and $b' \# x[b \mapsto y]$):

$$\begin{aligned}
& \text{elt}(z, a) [a \mapsto \text{atm}(b)] [b \mapsto y] \\
&= \text{elt}(z [a \mapsto \text{atm}(b)], b) [b \mapsto y] && \text{Figure 1}(\sigma \text{eltatm}) \\
&= (y@b') [b' \mapsto z\sigma] && \text{Figure 1}(\sigma \text{elta}) \\
&= (y@b') [b' \mapsto z\sigma'] && \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, a)), a \# y \\
&= (y@b') [a \mapsto \text{atm}(b) [b \mapsto y]] [b' \mapsto z\sigma'] && \text{Lemma 4.9, } a \# y@b' \\
&= (y@b') [b' \mapsto z [b \mapsto y]] [a \mapsto \text{atm}(b) [b \mapsto y]] && \text{IH } \text{level}(b') < \text{level}(b), b' \# x[b \mapsto y] \\
&= \text{elt}(z, a) [b \mapsto y] [a \mapsto \text{atm}(b) [b \mapsto y]] && \text{Figure 1}(\sigma \text{eltb})
\end{aligned}$$

— Suppose $x=[a'](x@a')$ for some fresh $a' \in \mathbb{A}^{i-1}$ (so $a' \# z, x, y$ and $k \leq \text{level}(a')$).

We reason as follows:

$$\begin{aligned}
& \text{elt}(z, a) [a \mapsto x] [b \mapsto y] = (x@a') [a' \mapsto z [a \mapsto x]] [b \mapsto y] && \text{Figure 1}(\sigma \text{elta}) \\
&= (x@a') [b \mapsto y] [a' \mapsto z\sigma] && \text{IH } k \leq \text{level}(a') = \text{level}(a) - 1, a' \# y \\
&= (x@a') [b \mapsto y] [a' \mapsto z\sigma'] && \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, a)), a \# y \\
&= (x[b \mapsto y]@a') [a' \mapsto z\sigma'] && \text{Lemma 4.11, } a' \# y \\
&= \text{elt}(z [b \mapsto y], a) [a \mapsto x] [b \mapsto y] && \text{Figure 1}(\sigma \text{elta}) \\
&= \text{elt}(z, a) [b \mapsto y] [a \mapsto x] [b \mapsto y] && \text{Figure 1}(\sigma \text{elta}), a \# y
\end{aligned}$$

— The case of $\text{elt}(z, c)$ for $k \in \mathbb{Z}$ and $c \in \mathbb{A}^k$ and $z \in \text{Set}^{k-1}$. We reason as follows:

$$\begin{aligned}
& \text{elt}(z, c) [a \mapsto x] [b \mapsto y] = \text{elt}(z\sigma, c) && \text{Figure 1}(\sigma \text{eltb}), \text{ twice} \\
&= \text{elt}(z\sigma', c) && \text{IH } \text{age}(z) < \text{age}(\text{elt}(z, a)), a \# y \\
&= \text{elt}(z, c) [b \mapsto y] [a \mapsto x] [b \mapsto y] && \text{Figure 1}(\sigma \text{eltb}), \text{ twice}
\end{aligned}$$

We consider the possibilities for $z \in \text{Set}^k$:

- If z is an internal atom then we reason using (σa) and (σb) of Figure 1.
- If z is an internal comprehension then we use Lemma 2.66(2) for a fresh $c \in \mathbb{A}^{k-1}$ (so $c \# z$), $(\sigma [])$, and the inductive hypothesis on $z@c$. \square

REMARK 4.13. Were Lemma 4.12 about the syntax of first-order logic or the λ -calculus, then it could be called *the substitution lemma*, and the proof would be a routine induction on syntax.

In fact, even in the case of first-order logic or the λ -calculus, the proof is not routine. Issues with binders (Figure 1 (σelta) , and one explicit in $(\sigma [])$) were the original motivation for the author's thesis [Gab01] and for nominal techniques in general. Our use of nominal techniques in this paper is more extensive and more interested in semantics; so nominal abstract syntax is present but more as a background technology than a stand-out feature.

For a standard non-rigorous non-nominal proof of the substitution lemma see [Bar84]; for a detailed discussion of the lemma in the context of Nominal Isabelle, see [Bar14] which includes many further references.

But the proof of Lemma 4.12 is not just a replay of the proofs; neither in the 'classic' sense of [Bar84] nor in the 'nominal' sense of [Gab01; Bar14]. This is because of the interaction of elt with the σ -action, mostly because of (σelta) (to a lesser extent also because of the nominal binder $(\sigma [])$).

COROLLARY 4.14 ((σswp)). Suppose $Z \in \text{Pred}$ and $k \in \mathbb{Z}$ and $z \in \text{Set}^k$. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and suppose $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $y \in \text{Set}^j$. Suppose $a \# y$ and $b \# x$. Then

$$\begin{aligned}
Z[a \mapsto x] [b \mapsto y] &= Z[b \mapsto y] [a \mapsto x] \\
z[a \mapsto x] [b \mapsto y] &= z[b \mapsto y] [a \mapsto x].
\end{aligned}$$

Proof. From Lemmas 4.12 and 4.9. \square

COROLLARY 4.15 ((σasc)). Suppose $Z \in \text{Pred}$ and $k \in \mathbb{Z}$ and $z \in \text{Set}^k$. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and suppose $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $y \in \text{Set}^j$. Suppose $a \# y$ and $b \# Z, z$.¹¹ Then

$$\begin{aligned} Z[a \mapsto x][b \mapsto y] &= Z[a \mapsto x][b \mapsto y] \\ z[a \mapsto x][b \mapsto y] &= z[a \mapsto x][b \mapsto y]. \end{aligned}$$

Proof. From Lemmas 4.12 and 4.9. □

4.3.4. (σid): *substitution for atoms and its corollaries.* We called $\text{atm}(a)$ in Definition 3.1 an *internal atom*. Atoms in nominal techniques interpret variables, so if we call $\text{atm}(a)$ an internal atom this should suggest that $\text{atm}(a)$ should behave like a variable (or a variable symbol). Rules (σa) and (σb) from Figure 1 are consistent with that, and Lemma 4.16 makes formal more of this intuition:

LEMMA 4.16 ((σid)). Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then:

- (1) If $Z \in \text{Pred}$ then $Z[a \mapsto \text{atm}(a)] = Z$.
- (2) If $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ then $z[a \mapsto \text{atm}(a)] = z$.

Proof. We reason by induction on $\text{age}(Z)$ and $\text{age}(z)$. We consider the possibilities for $Z \in \text{Pred}$:

- If $Z = \text{and}(\mathcal{Z})$ for $\mathcal{Z} \subseteq_{\text{fin}} \text{Pred}$ or $Z = \text{neg}(Z')$ for $Z' \in \text{Pred}$ then we use rules (σand) and (σneg) of Figure 1 and the inductive hypothesis.
- If $Z = \text{all}[a']Z'$ for $Z' \in \text{Pred}$ and $a' \in \mathbb{A}^{i'}$ for some $i' \in \mathbb{Z}$ then we use (σall) of Figure 1 and the inductive hypothesis.
- If $Z = \text{elt}(z, b)$ for $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and $z \in \text{Set}^{j-1}$ then we use rule (σeltb) of Figure 1 and the inductive hypothesis.
- If $Z = \text{elt}(z, a)$ for $z \in \text{Set}^{i-1}$ then we use (σeltatm) of Figure 1 and the inductive hypothesis for z .

We consider the possibilities for $z \in \text{Set}^k$:

- If z is an atom then we reason using (σa) or (σb) of Figure 1.
- If z is an internal comprehension then we use Lemma 2.66(2) for a fresh $c \in \mathbb{A}^{k-1}$ (so $c \# z$), ($\sigma[]$), and the inductive hypothesis on $z@c$. □

Given what we have so far, Lemma 4.17 is not hard to prove.

LEMMA 4.17 ((σren)). Suppose $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$. Then:

- If $Z \in \text{Pred}$ and $a' \# Z$ then $Z[a \mapsto \text{atm}(a')] = (a' a) \cdot Z$.
- If $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ and $a' \# z$ then $z[a \mapsto \text{atm}(a')] = (a' a) \cdot z$.

Proof. Suppose $Z \in \text{Pred}$ and $a' \# Z$. We note by Lemma 4.7(1) (since $a' \# Z$) that $Z[a \mapsto \text{atm}(a')] = ((a' a) \cdot Z)[a' \mapsto \text{atm}(a')]$ and use Lemma 4.16(1). The case of $z \in \text{Set}^k$ is exactly similar. □

5. THE DENOTATION OF AN INTERNAL PREDICATE AS A SET OF PREPOINTS

In this Section we study *prepoints* (Definition 5.3). In the notation of Definition 5.3, the intuition of $p = \{a \circ x \mid a \circ x \in p\} \in \text{PrPt}$ is a conjunction of assertions of the form ‘ x is an element of a ’ or ‘ $\text{elt}(x, a)$ ’.

This is the basic building block of predicates (see Definition 3.1) so it makes sense to build (pre)points out of them.

The main result of this Section is Theorem 5.17.

¹¹ We expect a stronger version of Corollary 4.15 to be possible in which we do not assume $a \# y$. However, the proof would require an induction resembling the proof of Lemma 4.12—the proof assuming $a \# y$ can piggyback on the induction already given in Lemma 4.12. We will not need this stronger version, so we do not bother.

(modand)	$p \models \text{and}(\mathcal{X}) \Leftrightarrow \forall X \in \mathcal{X}. p \models X$
(modneg)	$p \models \text{neg}(X) \Leftrightarrow p \not\models X$
(modall)	$p \models \text{all}[a]X \Leftrightarrow \forall a' \in \mathbb{A}^{\text{level}(a)}. p \models (a' a) \cdot X$
(modelt)	$p \models \text{elt}(x, a) \Leftrightarrow a \circ x \in p$
(modatm)	$\llbracket \text{atm}(a) \rrbracket^{\mathcal{P}} = [b] \{p \in \mathcal{P} \mid a \circ \text{atm}(b) \in p\}$
(modset)	$\llbracket [a]X \rrbracket^{\mathcal{P}} = [a] \{p \in \mathcal{P} \mid p \models X\}$

Fig. 3: The interpretation of internal predicates (Definition 5.4)

Prepoints are only preliminary. What we really need are *points*, which are prepoints subject to niceness conditions; see Section 8.

5.1. Prepoints and the denotation

Recall Set^i (internal sets) from Definition 3.1.

NOTATION 5.1. Define *Base* (as in **base predicates**) by

$$\text{Base} = \bigcup_{i \in \mathbb{Z}} \mathbb{A}^i \times \text{Set}^{i-1}.$$

We let α range over elements of *Base* and we may write α as $a \circ x$ where $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^{i-1}$.

REMARK 5.2. The intuition of $\alpha = a \circ x$ is that it has the meaning of ‘ $\text{elt}(x, a)$ ’, or in more standard notation ‘ $x \in a$ ’.

Since these internal predicates are in a sense the base case in Definition 3.1, we call the set of all α *Base*. Another name for these might be *Atomic*, for ‘atomic predicates’, but that might cause confusion with atoms.

DEFINITION 5.3. Define **prepoints** PrPt by

$$\text{PrPt} = \text{pset}(\text{Base}).$$

So a prepoint p is a subset of $\bigcup_{i \in \mathbb{Z}} \mathbb{A}^i \times \text{Set}^{i-1}$.

Recall *nomPset* the *small-supported powerset* from Definition 2.42, and the notion of an *equivariant set* from Definition 2.44 and Lemma 2.45:

- DEFINITION 5.4(1) Define a **validity** relation $p \models X$ between $p \in \text{PrPt}$ and $X \in \text{Pred}$ inductively by the rules (**modand**) to (**modelt**) in Figure 3. As is standard, we write $p \not\models X$ for $\neg(p \models X)$.
 (2) Given equivariant $\mathcal{P} \subseteq \text{PrPt}$, map each internal set $x \in \text{Set}$ to an atoms-abstraction $\llbracket x \rrbracket^{\mathcal{P}} \in [\mathbb{A}^{i-1}] \text{nomPset}(\mathcal{P})$, as specified by (**modatm**) and (**modset**) in Figure 3.

REMARK 5.5. Some further comments on Figure 3:

- (1) (**modand**) translates conjunction to conjunction and (**modneg**) translates negation to negation. No surprises here.
- (2) (**modall**) translates universal quantification to the new-quantifier from Definition 2.34. Using Lemma 4.17 we can rewrite (**modall**) to

$$p \models \text{all}[a]X \Leftrightarrow \forall a' \in \mathbb{A}^{\text{level}(a)}. p \models X[a \mapsto \text{atm}(a')].$$

That is: $\text{all}[a]X$ is valid when $X[a \mapsto \text{atm}(a')]$ for a new/fresh a' .

This might seem odd:

— We expect $\forall a. \phi \Rightarrow \phi$ to hold but $\forall a. \phi \Rightarrow \phi$ does not in general hold.

However, if p is a *point* (Definition 8.3) then $\forall a'. p \models (a' a) \cdot X$ will indeed imply $p \models X$. See Remark 8.13 and Lemma 8.14.

— \mathbb{N} is generally known to commute with conjunction, like \forall —but *also* with disjunction and negation, which \forall should not do.

However, this only holds for elements with small support. If elements do not have small support, then \mathbb{N} does not display this behaviour.

See Remark 5.7, Lemma 5.10, and Theorem 8.15.

- (3) (**modelt**) translates the assertion ‘ x is an element of a ’ to the set of points that contain $a \circ x$. This is an intensional definition: $\llbracket x \rrbracket^{\text{PrPt}} = \llbracket y \rrbracket^{\text{PrPt}}$ does not imply $p \models \text{elt}(x, a) \Leftrightarrow p \models \text{elt}(y, a)$. Extensionality will hold ... for points. See also Remark 8.17.
- (4) Rule (**modatm**) identifies $\text{atm}(a)$ with $[b]\text{elt}(\text{atm}(b), a)$, or in more traditional notation with $\{b \mid b \in a\}$, thus identifying $\text{atm}(a)$ with its extension.

We intend our semantics to be extensional (proofs in Subsection 8.3), so in fact this is the only possible option for (**modatm**).

If we look back to rules (ra) and (ratm) of Figure 4 (σelta) and (σeltatm) of Figure 1 (ratm) can be viewed as a special case of (σelta), and (σeltatm) can be viewed as a special case of (σelta) under this interpretation.

This duplication affects the proofs: for instance the cases for $y = \text{atm}(n)$ and $x = \text{atm}(n)$ in the proof of Lemma 4.12 are ‘morally’ duplicates of the case $y = [b'](y@b')$ and $x = [a'](x@a')$ —search for ‘There are two sub-cases’.

However, this price is worth paying: we do not take $\text{atm}(a)$ to be *sugar* for $[b]\text{elt}(\text{atm}(b), a)$, because this mentions $\text{atm}(b)$, which has a lower level. Since levels are in \mathbb{Z} this would lead to an infinite regression in some proofs. To be quite precise: we need $\text{atm}(a)$ to be primitive in the syntax so that we can define *minlevel* in Definition 4.4 and so argue inductively in Proposition 4.6, Lemma 4.12, and Proposition 7.5.¹²

- (5) Rule (**modset**) translates sets comprehension to a nominal atoms-abstraction. Though simple enough to write out, it is significant because:
- While we can emulate nominal atoms-abstraction in syntax (on the left) in ZF sets, it would be harder to do this in the semantics (on the right). So the fact that we can write this definition, relies on the nominal foundation on which this paper is based.
 - It says we can concentrate on the denotation of internal predicates; up to an abstracted atom, this is exactly the same thing as the denotation of internal sets.

LEMMA 5.6. *Definition 5.4 is well-defined. That is, in rule (**modset**) the choice of fresh $a \in \mathbb{A}^{i-1}$ (so $a \# s$), does not matter.*

Proof. From Lemma 2.67. □

REMARK 5.7. Why model \forall using \mathbb{N} ? Why in (**modall**) of Figure 3 do we not take the ‘obvious’ option that $p \models \text{all}[a]X$ when $\forall x.p \models X[a \mapsto x]$, or even at least $\forall a'.p \models X[a \mapsto \text{atm}(a')]$?

\mathbb{N} and $(a' a)$ are weaker and more elementary than \forall and $[a \mapsto \text{atm}(a')]$ or $[a \mapsto x]$, and so we have better properties that are more easily proved. This makes them systematically easier to work with. The reader can verify this by considering in detail what the **all** cases would become with the ‘obvious’ alternative definitions, in Theorem 5.17 and similar results (search for proofs using Lemma 5.10).

- Using \forall and $[a \mapsto x]$ seems hard because we have no control over the size of x , and this would destroy inductive quantities.
- Using \forall and $[a \mapsto \text{atm}(a')]$ also seems hard, because we would lose the very important Theorem 5.17.

See Remark 5.20: in the language of that remark, ‘for fresh a' ’ is *robust under small perturbations* whereas ‘for every a' ’ is not robust under small perturbations (and ‘for every x ’ is impredicative).

REMARK 5.8. If $x \in \text{Set}^i$ then $\llbracket x \rrbracket^P$ can be viewed as a kind of graph as follows:

¹²The author spent quite a while trying to make coinductive proofs work in which $\text{atm}(a)$ was literally identified with $[b]\text{elt}(\text{atm}(b), a)$ in the syntax (rather than just extensionally equal to it in the semantics).

- Nodes have the form $p \in \mathcal{P}$ or $\llbracket x \rrbracket^P$ for $x \in \text{Set}^i$.
- There is an edge labelled a from $\llbracket x \rrbracket^P$ to $p \in \mathcal{P}$ when $p \in \llbracket x \rrbracket^P @ a$.
- There is an edge labelled a from p to $\llbracket x' \rrbracket^P$ when $a \circ x \in p$.

Thus the denotation of Figure 3 can be thought of as a coinductive structure.

It is not *quite* a graph, because transitions out of $\llbracket x \rrbracket^P$ require us to generate a fresh name for the abstracted atom. Such transition systems are a natural nominal model for systems that can create new/local names, and were considered for the π -calculus in [Gab03]. Developing these is out of scope for this paper. It is still reasonable to say that the denotation of an internal predicate is a graph.

We do not make these intuitions formal in this paper; we do not develop a theory of graphs-with-name-generation and a general class of the models to which the concrete model of this paper belongs. Such an analysis would be very interesting, but it belongs to future work.

Coinductive ideas, though we leave it slightly implicit, exert a concrete technical influence on the mathematics in this paper: see for instance the duality evident in the design of Figure 4 and in Theorem 5.17, Proposition 6.11, and Lemma 12.24.

We conclude with some technical lemmas:

- (1) Lemma 5.9 states what Notation 3.8 strongly suggests must hold.
- (2) Lemma 5.10 unpacks the internal universal quantifier all to a \mathcal{N} -quantifier—but see Theorem 8.15.
- (3) Lemma 5.11, which is not hard to prove, can be viewed as a *TI* property in the topological sense [Wil70, Definition 13.3], that distinct points can be separated by some internal predicate X (thought of as an ‘open set’).

LEMMA 5.9. *Suppose $X, Y \in \text{Pred}$ and $p \in \text{PrPt}$. Then:*

- (1) $p \models \text{imp}(X, Y)$ if and only if $p \models X \Rightarrow p \models Y$.
- (2) $p \models \text{iff}(X, Y)$ if and only if $p \models X \Leftrightarrow p \models Y$.
- (3) $p \not\models \text{false}$ and $p \models \text{true}$.

Proof. From Notation 3.8 and Example 3.9 by sets calculations with (**modand**) and (**modneg**) from Figure 3. \square

LEMMA 5.10. *Suppose $X \in \text{Pred}$ and $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then the following are equivalent:*

$$p \models \text{all}[a]X \Leftrightarrow \forall a' \in \mathbb{A}^i. p \models (a' \ a) \cdot X \Leftrightarrow \forall a' \in \mathbb{A}^i. (a' \ a) \cdot p \models X.$$

Proof. The first equivalence just repeats Figure 3 (**modall**). The second equivalence follows by Theorem 2.31. \square

LEMMA 5.11. *Suppose $p, q \in \text{PrPt}$. Then*

$$\forall X \in \text{Pred}. (p \models X \Leftrightarrow q \models X) \text{ implies } p = q.$$

Proof. Assume $p \models X$ if and only if $q \models X$ for any $X \in \text{Pred}$. To prove $p = q$ it suffices to prove that for any $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^{i-1}$ we have $a \circ x \in p \Leftrightarrow a \circ x \in q$. We reason as follows:

$$\begin{aligned} a \circ x \in p &\Leftrightarrow p \models \text{elt}(x, a) && \text{Figure 3(modelt)} \\ &\Leftrightarrow q \models \text{elt}(x, a) && \text{Assumption} \\ &\Leftrightarrow a \circ x \in q && \text{Figure 3(modelt)} \end{aligned}$$

\square

5.2. The amgis-action on prepoints

REMARK 5.12. The \circ -action (amgis-action) $p[u \leftarrow a]$ is a dual (adjoint) to the σ -action $X[a \mapsto u]$: this is made formal in Theorem 5.17; see also Proposition 6.11 and Lemma 12.24.

The idea of the \circ -action comes from previous work [Gab14; Gab16; GG16]. It is just as useful to us here.

$$\begin{array}{ll}
(\text{tb}) & boy \in p[x \leftarrow a] \Leftrightarrow bo(y[a \mapsto x]) \in p \\
(\text{ta}) & aoy \in p[[a']X \leftarrow a] \Leftrightarrow p \models X[a' \mapsto y[a \mapsto x]] \\
(\text{t atm}) & aoy \in p[\text{atm}(n) \leftarrow a] \Leftrightarrow no(y[a \mapsto \text{atm}(n)]) \in p
\end{array}$$

Fig. 4: The amgis-action (Definition 5.13)

DEFINITION 5.13. Then define an t -**action** (amgis-action) by the rules in Figure 4, where in that figure:

- $p \in \text{PrPt}$.
- $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ for some $i \in \mathbb{Z}$.
- $b \in \mathbb{A}^j$ and $y \in \text{Set}^{j-1}$ for some $j \in \mathbb{Z}$.
- In rule (ta) $X \in \text{Pred}$ and we assume $i=j$ and $a' \in \mathbb{A}^{i-1}$.
- In rule (t atm) $n \in \mathbb{A}^i$ is some atom not necessarily distinct from a .

REMARK 5.14. If we are willing to anticipate $v \in u$ from Notation 6.1, whose intuitive meaning as ‘ v is an element of u ’ should be quite clear, then we can use (modelt) from Figure 3 to simplify Figure 4 to this:

$$\begin{array}{ll}
p[x \leftarrow a] \models y \in b & \Leftrightarrow p \models y[a \mapsto x] \in b \\
p[x \leftarrow a] \models y \in a & \Leftrightarrow p \models y[a \mapsto x] \in x
\end{array}$$

Written thus, Figure 4 looks like base cases for Theorem 5.17—which is precisely what it is.

LEMMA 5.15. (ta) from Figure 4 is well-defined. That is, the choice of fresh $a' \in \mathbb{A}^{i-1}$ does not matter in $(u @ a')[a' \mapsto y[a \mapsto u]]$.

Proof. From Lemma 4.7(1) (property $(\sigma\alpha)$). □

The t -action maps prepoints to prepoints:

LEMMA 5.16. If $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ then $p[x \leftarrow a] \in \text{PrPt}$.

Proof. By construction in Definition 5.13 $p[x \leftarrow a] \subseteq \text{Base}$. □

5.3. Proof that amgis is dual to sigma

As discussed in Remark 5.12 we now prove that t is dual to σ . This is Theorem 5.17; this follows results such as [Gab16, Proposition 3.4.2(1)]. It states that the t -action behaves as a dual (a ‘left adjoint’) to the σ -action on internal predicates.

Theorem 5.17 may also appear as a definition; see for instance [Gab16, Definition 3.4.1]. Here it is a Theorem, because we start from a concrete model and deriving its properties. Thus, Theorem 5.17 is also a sanity check relative to previous material such as [Gab16; GG16; Gab14].

THEOREM 5.17. Suppose $p \in \text{PrPt}$ and $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then

$$p \models X[a \mapsto x] \quad \text{if and only if} \quad p[x \leftarrow a] \models X.$$

Proof. By induction on $\text{age}(X)$. We consider the possibilities for $X \in \text{Pred}$:

- *The case of $\text{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{\text{fm}} \text{Pred}$.* We reason as follows:

$$\begin{array}{ll}
p \models \text{and}(\mathcal{X})[a \mapsto x] & \Leftrightarrow p \models \text{and}(\{X[a \mapsto x] \mid X \in \mathcal{X}\}) \quad \text{Figure 1}(\sigma\text{and}) \\
& \Leftrightarrow \forall X \in \mathcal{X}. p \models X[a \mapsto x] \quad \text{Figure 3}(\text{modand}) \\
& \Leftrightarrow \forall X \in \mathcal{X}. p[x \leftarrow a] \models X \quad \text{IH } \text{age}(X) < \text{age}(\text{and}(\mathcal{X}))
\end{array}$$

— *The case of $\text{neg}(X)$.* We reason as follows:

$$\begin{aligned}
p \models \text{neg}(X)[a \mapsto x] &\Leftrightarrow p \models \text{neg}(X[a \mapsto x]) && \text{Figure 1}(\sigma\text{neg}) \\
&\Leftrightarrow p \not\models X[a \mapsto x] && \text{Figure 3}(\text{modneg}) \\
&\Leftrightarrow p[x \leftarrow a] \not\models X && \text{IH } \text{age}(X) < \text{age}(\text{neg}(X)) \\
&\Leftrightarrow p[x \leftarrow a] \models \text{neg}(X) && \text{Figure 3}(\text{modneg})
\end{aligned}$$

— *The case of $\text{all}[b]X$ where $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.* Using Lemma 3.7(1) assume without loss of generality that b is fresh (so $b \# x$). Note by Theorem 2.31 and Corollary 2.28(1) (since $b', b \# x, a$) that $(b' b) \cdot (p[x \leftarrow a]) = ((b' b) \cdot p)[x \leftarrow a]$. We reason as follows:

$$\begin{aligned}
p \models (\text{all}[b]X)[a \mapsto x] &\Leftrightarrow p \models \text{all}[b](X[a \mapsto x]) && \text{Figure 1}(\sigma\text{all}) \ b \# x \\
&\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' b) \cdot p \models X[a \mapsto x] && \text{Lemma 5.10} \\
&\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' b) \cdot (p[x \leftarrow a]) \models X && \text{IH } \text{age}(X) < \text{age}(\text{all}[b]X) \\
&\Leftrightarrow p[x \leftarrow a] \models \text{all}[b]X && \text{Lemma 5.10}
\end{aligned}$$

— *The case of $\text{elt}(y, b)$ for some $j \in \mathbb{Z}$ and $y \in \text{Set}^{j-1}$ and $b \in \text{Set}^j$.* We reason as follows:

$$\begin{aligned}
p \models \text{elt}(y, b)[a \mapsto x] &\Leftrightarrow p \models \text{elt}(y[a \mapsto x], b) && \text{Figure 1}(\sigma\text{eltb}) \\
&\Leftrightarrow b \circ (y[a \mapsto x]) \in p && \text{Figure 3}(\text{modelt}) \\
&\Leftrightarrow b \circ y \in p[x \leftarrow a] && \text{Figure 4}(\text{tb}) \\
&\Leftrightarrow p[x \leftarrow a] \models \text{elt}(y, b) && \text{Figure 3}(\text{modelt})
\end{aligned}$$

— *The case of $\text{elt}(y, a)$ for $i \in \mathbb{Z}$ and $y \in \text{Set}^{i-1}$.* There are two sub-cases:

— *Suppose $x = \text{atm}(n)$ for some $n \in \mathbb{A}^i$.* We reason as follows:

$$\begin{aligned}
p \models \text{elt}(y, a)[a \mapsto \text{atm}(n)] &\Leftrightarrow p \models \text{elt}(y[a \mapsto \text{atm}(n)], n) && \text{Figure 1}(\sigma\text{eltatm}) \\
&\Leftrightarrow n \circ (y[a \mapsto \text{atm}(n)]) \in p && \text{Figure 3}(\text{modelt}) \\
&\Leftrightarrow a \circ y \in p[\text{atm}(n) \leftarrow a] && \text{Figure 4}(\text{ratm}) \\
&\Leftrightarrow p[\text{atm}(n) \leftarrow a] \models \text{elt}(y, a) && \text{Figure 3}(\text{modelt})
\end{aligned}$$

— *Suppose $x = [b](x @ b)$ for some fresh $b \in \mathbb{A}^{i-1}$ (so $b \# x, y, a$).* We reason as follows:

$$\begin{aligned}
p \models \text{elt}(y, a)[a \mapsto x] &\Leftrightarrow p \models (x @ b)[b \mapsto y[a \mapsto x]] && \text{Figure 1}(\sigma\text{elta}) \\
&\Leftrightarrow a \circ y \in p[x \leftarrow a] && \text{Figure 4}(\text{ra}) \\
&\Leftrightarrow p[x \leftarrow a] \models \text{elt}(y, a) && \text{Figure 3}(\text{modelt}) \quad \square
\end{aligned}$$

REMARK 5.18. Theorem 5.17 resembles [Gab16, Proposition 3.4.2(1)] but there are differences.

First, the proof here is different. This is natural since the information going into the proofs is different. This paper concerns a concrete model of whose internal structure we have full knowledge, whereas [Gab16] concerns nominal algebras about which we only know abstract (nominal) algebraic properties.

Secondly, Theorem 5.17 is a stronger result. Again, this is because we are dealing with a concrete model, and we can ‘look inside’ it and take advantage of its specific structure. We place the results side-by-side in the notation of this paper:

$$\begin{array}{ll}
\text{[Gab16, Proposition 3.4.2(1)] asserts} & \forall p. \forall a. \forall X. (p \models X[a \mapsto x] \Leftrightarrow p[x \leftarrow a] \models X) \\
\text{Theorem 5.17 asserts} & \forall p. \forall a. \forall X. (p \models X[a \mapsto x] \Leftrightarrow p[x \leftarrow a] \models X).
\end{array}$$

REMARK 5.19. It might help to draw an analogy between Theorem 5.17 and a standard result in ordinary (non-nominal) denotational semantics:

Imagine ϕ is a formula and s is a term in first-order logic, and that we give formulas and terms a denotational semantics in sets. Then we expect that $\llbracket \phi[a \mapsto s] \rrbracket_\varsigma = \llbracket \phi \rrbracket_{\varsigma[a \mapsto [s]]}$: the model of ϕ with a substituted for s in a valuation ς is equal to the model of ϕ in the valuation ς where a maps to the model of s .

Theorem 5.17 corresponds to this, where p plays the role of ς . So points p are analogous to valuation contexts—though p is also more than a valuation context: it does not evaluate atoms to denotations; even if it did, it evaluates to *nominal* elements, which can be incomplete in the sense of having non-empty support; and p may be subject to filter-like conditions, as we will discuss in Section 8.

REMARK 5.20. It is worth pausing to note in Theorem 5.17 the treatment of quantification \forall . Recall from Remark 5.7 the discussion of why we model \forall using \mathbb{I} . We can write informally that $\forall = \mathbb{I}$ (see (modall) in Figure 3 for the precise statement).

If following Remark 5.19 we think of p as like a valuation ς , and of $p[u \leftarrow a]$ as like $\varsigma[a := \llbracket u \rrbracket_\varsigma]$ (p with a reassigned to the meaning of u in p)—then we see that modelling \forall using ‘for every atom’ is incompatible with Theorem 5.17, because reassigning *one* atom in p might change a universal quantification over all atoms from being true, to being false.

\mathbb{I} has different behaviour: reassigning the meaning of one atom, or any small (Notation 2.6) number of atoms, does not affect the meaning of \mathbb{I} , since it means ‘for all but a small number of atoms’. Thus we can say that our model of \forall using \mathbb{I} is **robust under small perturbations** of p . So note that Theorem 5.17 depends on $\forall = \mathbb{I}$. We see something similar in Definition 12.37, where we reassign meanings given to a small set of atoms with respect to a prepoint $herb(ext)$, and this is ‘safe’ with respect to universal quantifiers.

For more on how \mathbb{I} can, if the prepoint is suitably well-behaved, fully and correctly model \forall , see Definition 8.1, Remark 8.2, and Theorem 8.15.

6. SOME SUGAR, AND ITS PROPERTIES

In this section we set up various important notations and definitions and prove their basic properties. The common theme is ‘being an element of’. Technical highlights are:

- $y \in x$ in Notation 6.1 which as we would imagine internalises “ y is an element of x ”.
- px in Definition 6.2 which expresses intuitively what “ y is an element of x ” looks like from a specific prepoint.
- The important Lemma 6.6, that $(y \in x)[a \mapsto u] = y[a \mapsto u] \in (x[a \mapsto u])$.
- Proposition 6.17 makes formal how $y \in x$ interacts with int , cmp , and every from Notation 6.14.

6.1. Prepoints as maps from internal sets to sets of internal sets

The main definition of this Subsection is Definition 6.2, which notes that $p \in \text{PrPt}$ induces a denotation for an internal set $x \in \text{Set}^i$ as a set of (internal) sets. This will help define *points* in Definition 8.3.

6.1.1. *The basic definition.* Some notation will be useful:

NOTATION 6.1.— Suppose $i \in \mathbb{Z}$ and $x \in \text{Set}^i$ is an internal comprehension¹³ and $y \in \text{Set}^{i-1}$. Then define $y \in x$ by

$$y \in x = (x @ b)[b \mapsto y]$$

where we choose $b \in \mathbb{A}^{i-1}$ fresh (so $b \# x, y$).

- Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $y \in \text{Set}^{i-1}$. Then define $y \in \text{atm}(a)$ by

$$y \in \text{atm}(a) = \text{elt}(y, a).$$

- Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $b \in \mathbb{A}^{i-1}$ and $x \in \text{Set}^i$ and $y \in \text{Set}^{i-1}$. Then define $y \in a$, $b \in x$, and $b \in a$ by:

$$\begin{aligned} y \in a &= \text{elt}(y, a) \\ b \in x &= \text{atm}(b) \in x \\ b \in a &= \text{atm}(b) \in a = \text{elt}(\text{atm}(b), a) \end{aligned}$$

Recall the notation $p \models X$ from Figure 3:

¹³Terminology from Notation 3.2. So x has the form $[b](x @ b)$ for some $b \in \mathbb{A}^{i-1}$ with $b \# x$, and x does not have the form $\text{atm}(a)$ for any $a \in \mathbb{A}^{i-1}$.

DEFINITION 6.2. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then define $p(a)$ and $p(x)$ by:

$$\begin{aligned} p(a) &= \{y \in \text{Set}^{i-1} \mid a \circ y \in p\} \\ p(x) &= \{y \in \text{Set}^{i-1} \mid p \models y \in x\} \end{aligned}$$

Later on, we may drop brackets and write pa for $p(a)$ and px for $p(x)$.

Lemma 6.3 is a useful result and serves as a sanity check that $p(a)$ from the first line of Definition 6.2 coincides with $p(\text{atm}(a))$ from the second line, so the first clause is in a natural sense a special case of the second:

LEMMA 6.3. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$p(a) = p(\text{atm}(a)).$$

Proof. We reason as follows:

$$\begin{aligned} y \in p(\text{atm}(a)) &\Leftrightarrow p \models y \in \text{atm}(a) && \text{Definition 6.2, } p(x) \text{ clause} \\ &\Leftrightarrow p \models \text{elt}(y, a) && \text{Notation 6.1} \\ &\Leftrightarrow a \circ y \in p && \text{Figure 3(modelt)} \\ &\Leftrightarrow y \in p(a) && \text{Definition 6.2, } p(a) \text{ clause} \end{aligned} \quad \square$$

REMARK 6.4. The rest of this Subsection collects some technical results. We briefly survey them:

- Lemma 6.5 connects Notation 6.1 with the σ -action on $X \in \text{Pred}$.
- Lemma 6.6 and Corollary 6.7 check that the σ -action distributes correctly through Notation 6.1.
- Lemma 6.8 checks $y \in x$ coincides with atoms-concretion, if y is an internal atom fresh for x .
- Proposition 6.11 resembles Theorem 5.17 in relating \triangleright and σ , but it does this for $p(-)$. This result will be useful, but it is also interesting just in itself.
- Corollary 6.13 will be useful and is obtained using Lemmas 6.12 and 6.6.

6.1.2. Syntactic lemmas

LEMMA 6.5. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and $a \# x$. Then (using Notation 6.1)

$$x \in [a]X = X[a \mapsto x].$$

Proof. Note by Lemma 2.63 that $a \# [a]X$. By Notation 6.1 (since $a \# x$, $[a]X$) $x \in [a]X$ is equal to $(([a]X) @ a)[a \mapsto x]$ and by Lemma 2.66(1) this is equal to $X[a \mapsto x]$. \square

LEMMA 6.6. Suppose $i, j \in \mathbb{Z}$ and $x \in \text{Set}^{i+1}$ and $y \in \text{Set}^i$ and $a \in \mathbb{A}^j$ and $u \in \text{Set}^j$. Then:

- (1) $(y \in x)[a \mapsto u] = y[a \mapsto u] \in x[a \mapsto u]$.
- (2) $(y \in a)[a \mapsto u] = y[a \mapsto u] \in u$, where $j = i+1$.
- (3) $(y \in b)[a \mapsto u] = y[a \mapsto u] \in b$, where $b \in \mathbb{A}^{i+1}$.

Proof. First, suppose we have proved part 1 of this result. Then part 2 follows using Figure 1 (σa) and part 3 follows using Figure 1 (σb).

To prove part 1 there are three cases:

- Suppose $x = \text{atm}(a')$ for some $a' \in \mathbb{A}^{i+1}$ not equal to a .

We reason as follows:

$$\begin{aligned} (y \in \text{atm}(a'))[a \mapsto u] &= \text{elt}(y, a')[a \mapsto u] && \text{Notation 6.1} \\ &= \text{elt}(y[a \mapsto u], a') && \text{Figure 1}(\sigma \text{eltb}) \\ &= y[a \mapsto u] \in \text{atm}(a') && \text{Notation 6.1} \\ &= y[a \mapsto u] \in (\text{atm}(a')[a \mapsto u]) && \text{Figure 1}(\sigma b) \end{aligned}$$

- Suppose $x = \text{atm}(a)$ (so that $j = i+1$).

There are two sub-cases:

— Suppose $u = \text{atm}(n)$ for some $n \in \mathbb{A}^i$. We reason as follows:

$$\begin{aligned} (y \in \text{atm}(a))[a \mapsto \text{atm}(n)] &= \text{elt}(y, a)[a \mapsto \text{atm}(n)] && \text{Notation 6.1} \\ &= \text{elt}(y[a \mapsto \text{atm}(n)], n) && \text{Figure 1}(\sigma \text{eltatm}) \\ &= y[a \mapsto \text{atm}(n)] \in \text{atm}(n) && \text{Notation 6.1} \end{aligned}$$

— Suppose $u = [a'](u @ a')$ for some fresh $a' \in \mathbb{A}^{i-1}$ (so $a' \# u, y$). We reason as follows:

$$\begin{aligned} (y \in \text{atm}(a))[a \mapsto u] &= \text{elt}(y, a)[a \mapsto u] && \text{Notation 6.1} \\ &= (u @ a')[a' \mapsto y[a \mapsto u]] && \text{Figure 1}(\sigma \text{elta}) \\ &= y[a \mapsto u] \in u && \text{Notation 6.1} \end{aligned}$$

— Suppose x is an internal comprehension (not an internal atom).

Choose $b \in \mathbb{A}^i$ fresh (so $b \# x, y, u$). We reason as follows:

$$\begin{aligned} (y \in x)[a \mapsto u] &= (x @ b)[b \mapsto y][a \mapsto u] && \text{Notation 6.1} \\ &= (x @ b)[a \mapsto u][b \mapsto y[a \mapsto u]] && \text{Lemma 4.12 } b \# u \\ &= (x[a \mapsto u] @ b)[b \mapsto y[a \mapsto u]] && \text{Lemma 4.11 } b \# x, u \\ &= y[a \mapsto u] \in x[a \mapsto u] && \text{Notation 6.1} \end{aligned} \quad \square$$

COROLLARY 6.7. Suppose $k \in \mathbb{Z}$ and $c \in \mathbb{A}^k$ and $x \in \text{Set}^k$ and $y \in \text{Set}^{k-1}$ and $c \# y$. Then

$$\text{if } z = [c](y \in c) \in \text{Set}^{k+1} \text{ then } x \in z = y \in x.$$

Proof. We reason as follows:

$$\begin{aligned} x \in z &= x \in [c](y \in c) && \text{Assumption} \\ &= (y \in c)[c \mapsto x] && \text{Lemma 6.5} \\ &= y[c \mapsto x] \in x && \text{Lemma 6.6(1)} \\ &= y \in x && \text{Lemma 4.9 } c \# y \end{aligned} \quad \square$$

6.1.3. Semantic lemmas. We never use Lemma 6.8 directly, but we retain it as a sanity check:

LEMMA 6.8. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $x \in \text{Set}^i$ is an internal comprehension and $a \in \mathbb{A}^{i-1}$ and $a \# x$. Then

$$p \models a \in x \Leftrightarrow p \models x @ a.$$

Proof. We use Lemma 2.66(2) to write x as $[a](x @ a)$ and unfold Notation 6.1 and use Lemma 4.16:

$$p \models a \in x \Leftrightarrow p \models x @ a[a \mapsto \text{atm}(a)] \Leftrightarrow p \models x @ a. \quad \square$$

Lemma 6.9 is a kind of sequel to Lemma 6.3:

LEMMA 6.9. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $x \in \mathbb{A}^i$ and $b \in \mathbb{A}^{i-1}$ and $b \# u$. Then

$$p(u) = p([b](b \in u)).$$

Proof. We reason as follows:

$$\begin{aligned} y \in p([b](b \in u)) &\Leftrightarrow p \models y \in [b](b \in u) && \text{Definition 6.2, } p(x) \text{ clause} \\ &\Leftrightarrow p \models (b \in u)[b \mapsto y] && \text{Lemma 6.5} \\ &\Leftrightarrow p \models (b[b \mapsto y]) \in (u[b \mapsto y]) && \text{Lemma 6.6(1)} \\ &\Leftrightarrow p \models y \in u && \text{Figure 1}(\sigma \mathbf{a}), \text{ Lemma 4.9 } b \# u \\ &\Leftrightarrow y \in p(u) && \text{Definition 6.2, } p(x) \text{ clause} \end{aligned} \quad \square$$

Lemma 6.10 will be useful for Proposition 6.11:

LEMMA 6.10. Suppose $i, j \in \mathbb{Z}$ and $x \in \text{Set}^{i+1}$ and $y \in \text{Set}^i$ and $a \in \mathbb{A}^j$ and $u \in \text{Set}^j$. Suppose $p \in \text{PrPt}$. Then

$$p[u \leftarrow a] \models y \in x \Leftrightarrow p \models y[a \mapsto u] \in (x[a \mapsto u]).$$

Proof. Combining Lemma 6.6(1) with Theorem 5.17. \square

PROPOSITION 6.11. *Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $u \in \text{Set}^i$. Suppose $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ and $y \in \text{Set}^{k-1}$. Then:*

$$\begin{aligned} a \# z &\Rightarrow y \in p[u \leftarrow a](z) \Leftrightarrow y[a \rightarrow u] \in p(z) \\ pu = pa \wedge k = i &\Rightarrow y \in p[u \leftarrow a](a) \Leftrightarrow y[a \rightarrow u] \in p(a) \end{aligned}$$

Proof. We unpack Definition 6.2 and reason as follows:

$$\begin{aligned} y \in p[u \leftarrow a](z) &\Leftrightarrow p[u \leftarrow a] \models y \in z && \text{Definition 6.2} \\ &\Leftrightarrow p \models y[a \rightarrow u] \in z[a \rightarrow u] && \text{Lemma 6.6(1)} \\ &\Leftrightarrow p \models y[a \rightarrow u] \in z && \text{Lemma 4.9, } a \# z \\ &\Leftrightarrow y[a \rightarrow u] \in pz && \text{Definition 6.2} \\ \\ y \in p[u \leftarrow a](a) &\Leftrightarrow p[u \leftarrow a] \models y \in a && \text{Definition 6.2} \\ &\Leftrightarrow p \models y[a \rightarrow u] \in u && \text{Lemmas 6.10 \& 6.6(2)} \\ &\Leftrightarrow p \models y[a \rightarrow u] \in a && \text{Definition 6.2, } pu = pa \\ &\Leftrightarrow y[a \rightarrow u] \in pa && \text{Definition 6.2} \end{aligned} \quad \square$$

Recall from Definition 3.11 the definitions of empt and set :

LEMMA 6.12. *Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $y \in \text{Set}^{i-1}$. Then*

$$p \not\models y \in \text{empt}^i \quad \text{and} \quad p \models y \in \text{set}^i.$$

As a corollary,

$$p \not\models \text{set}^{i-1} \in \text{empt}^i \quad \text{and} \quad p \models \text{set}^{i-1} \in \text{set}^i.$$

Proof. We reason as follows, where $p \in \text{PrPt}$ and $a \in \text{Set}^{i-1}$:

$$\begin{aligned} p \models y \in \text{empt}^i &\Leftrightarrow p \models y \in [a] \text{false} && \text{Definition 3.11} \\ &\Leftrightarrow p \models \text{false}[a \rightarrow y] && \text{Notation 6.1} \\ &\Leftrightarrow p \models \text{false} && \text{Corollary 4.10} \\ &\Leftrightarrow \perp && \text{Lemma 5.9(3)} \end{aligned}$$

The case of set^i is almost identical and for the corollary we just take $y = \text{set}^{i-1}$. \square

COROLLARY 6.13. *Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$. Then*

$$p(\text{empt}^i) = \emptyset \quad \text{and} \quad p(\text{set}^i) = \text{Set}^{i-1}.$$

Proof. This just rephrases Lemma 6.12 using Definition 6.2. \square

6.2. Operations on internal sets

In Proposition 6.17 we wrap and and neg in an internal comprehension $[a]$ - and so check the behaviour of internal sets analogues int and cmp .¹⁴ We then exploit the nominal syntax and semantics to do the same for all and every , the universal quantifications on internal predicates and internal sets.

6.2.1. Intersection, complement, and ‘every’ on internal sets. Recall from Notation 3.2 that every internal set is either an internal atom $\text{atm}(a)$ or an internal comprehension $[a]X$. Notation 6.14 gives some natural ways to build new internal sets out of old ones:

NOTATION 6.14. Suppose $i \in \mathbb{Z}$. We define the following notation:

¹⁴In ZF set theory we can do this for and but not (unrestrictedly) for neg , so this simple observation has some content.

— Suppose $\mathcal{Z} \subseteq_{\text{fin}} \text{Set}^i$ is a finite set of internal comprehensions and $a \in \mathbb{A}^{i-1}$ and $a \# \mathcal{Z}$, so that by Lemma 2.49(3) also $a \# z$ for every $z \in \mathcal{Z}$. Then we write

$$\begin{aligned} \text{int}(\mathcal{Z}) &= [a] \text{and}(\{z @ a \mid z \in \mathcal{Z}\}) \quad \text{and} \\ \text{uni}(\mathcal{Z}) &= [a] \text{or}(\{z @ a \mid z \in \mathcal{Z}\}). \end{aligned}$$

— Suppose $z \in \text{Set}^i$ is an internal comprehension and $a \in \mathbb{A}^{i-1}$ and $a \# z$. Then we write

$$\text{cmp}(z) = [a] \text{neg}(z @ a).$$

— Suppose $z \in \text{Set}^i$ is an internal comprehension and $k \in \mathbb{Z}$ and $c \in \mathbb{A}^k$ and $a \in \mathbb{A}^{i-1}$ and $a \# z$. Then we write

$$\text{every}[c]z = [a] \text{all}[c](z @ a).$$

Notation 6.14 is well-defined by Lemma 2.67.

REMARK 6.15. As int and cmp from Notation 6.14 are operations on internal sets corresponding to conjunction and negation, so every corresponds to quantification; this is made formal in Proposition 6.17.

We illustrate every intuitively by taking $z = [a]Z$ so that $\text{every}[c][a]Z = [a] \text{all}[c]Z$. For example:

$$\text{every}[a]([d] \text{iff}(\text{elt}(a, c), \text{elt}(a, d))) = [d] \text{all}[a] \text{iff}(\text{elt}(a, c), \text{elt}(a, d)).$$

If we switch to a less formal notation we write that

$$\text{every } a.(\{d \mid a \in c \Leftrightarrow a \in d\}) \quad \text{equals} \quad \{d \mid \forall a. a \in c \Leftrightarrow a \in d\}$$

—or more succinctly, that

$$\text{every } a.(\{d \mid a \in c \Leftrightarrow a \in d\}) \quad \text{equals} \quad \{c\}.$$

LEMMA 6.16(1) $\text{int}(\mathcal{X})[a \mapsto u] = \text{int}(\{x[a \mapsto u] \mid x \in \mathcal{X}\})$

(2) $\text{cmp}(x)[a \mapsto u] = \text{cmp}(x[a \mapsto u])$

(3) If $a' \# u$ then $(\text{every}[a']x)[a \mapsto u] = \text{every}[a'](x[a \mapsto u])$.

Proof. By routine calculations using Lemma 2.64 and (σand) , (σneg) , (σall) , and $(\sigma [])$. \square

6.2.2. Interaction with the sigma-action

PROPOSITION 6.17. Suppose $k \in \mathbb{Z}$ and $x \in \text{Set}^{k-1}$ and $p \in \text{Pnt}$. Then:

(1) If $\mathcal{Z} \subseteq_{\text{fin}} \text{Set}^k$ is a finite set of internal comprehensions (Notation 3.2) then

$$\begin{aligned} p \models x \in \text{int}(\mathcal{Z}) &\Leftrightarrow \forall z' \in \mathcal{Z}. p \models x \in z' \quad \text{and} \\ p \models x \in \text{uni}(\mathcal{Z}) &\Leftrightarrow \exists z' \in \mathcal{Z}. p \models x \in z'. \end{aligned}$$

(2) If $z \in \text{Set}^k$ is an internal comprehension then

$$p \models x \in \text{cmp}(z) \Leftrightarrow p \not\models x \in z.$$

(3) If $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $z \in \text{Set}^k$ is an internal comprehension and $a \# z$ then

$$\begin{aligned} p \models x \in \text{every}[a]z &\Leftrightarrow p \models \text{all}[a](x \in z) \\ &\Leftrightarrow \forall a' \in \mathbb{A}^i. (a' a). p \models x \in z. \end{aligned}$$

Proof. (1) Choose $c' \in \mathbb{A}^{k-1}$ fresh (so $c' \# x$ and $c' \# z'$ for every $z' \in \mathcal{Z}$). We reason as follows:

$$\begin{aligned} p \models x \in \text{int}(\mathcal{Z}) &\Leftrightarrow p \models (([c'] \text{and}(\{z' @ c' \mid z' \in \mathcal{Z}\})) @ c')[c' \mapsto x] && \text{Notations 6.14 \& 6.1} \\ &\Leftrightarrow p \models \text{and}(\{z' @ c' \mid z' \in \mathcal{Z}\})[c' \mapsto x] && \text{Lemma 2.66(1)} \\ &\Leftrightarrow p \models \text{and}(\{(z' @ c')[c' \mapsto x] \mid z' \in \mathcal{Z}\}) && \text{Figure 1}(\sigma \text{and}) \\ &\Leftrightarrow p \models \text{and}(\{x \in z' \mid z' \in \mathcal{Z}\}) && \text{Notations 6.14 \& 6.1} \\ &\Leftrightarrow \forall z' \in \mathcal{Z}. p \models x \in z' && \text{Figure 3}(\text{modand}) \end{aligned}$$

The case of uni is similar.

(2) Choose $c' \in \mathbb{A}^{k-1}$ fresh (so $c' \# x, z$). We reason as follows:

$$\begin{aligned}
 p \models x \in \text{cmp}(z) &\Leftrightarrow p \models (([c'] \text{neg}(z @ c')) @ c')[c' \mapsto x] && \text{Notations 6.14 \& 6.1} \\
 &\Leftrightarrow p \models \text{neg}(z @ c')[c' \mapsto x] && \text{Lemma 2.66(1)} \\
 &\Leftrightarrow p \models \text{neg}((z @ c')[c' \mapsto x]) && \text{Figure 1}(\sigma \text{neg}) \\
 &\Leftrightarrow p \not\models (z @ c')[c' \mapsto x] && \text{Figure 3}(\text{modneg}) \\
 &\Leftrightarrow p \not\models x \in z && \text{Notations 6.14 \& 6.1}
 \end{aligned}$$

(3) Choose $c \in \mathbb{A}^{k-1}$ fresh (so $c \# x, z$). We reason as follows:

$$\begin{aligned}
 p \models x \in \text{every}[a]z &\Leftrightarrow p \models x \in [c] \text{all}[a](z @ c) && \text{Notation 6.14} \\
 &\Leftrightarrow p \models (\text{all}[a](z @ c))[c \mapsto x] && \text{Notation 6.1} \\
 &\Leftrightarrow p \models \text{all}[a]((z @ c)[c \mapsto x]) && \text{Figure 1}(\sigma \text{all}) \ a \# x \\
 &\Leftrightarrow p \models \text{all}[a](x \in z) && \text{Notation 6.1} \\
 &\Leftrightarrow \forall a' \in \mathbb{A}^i. (a' \ a) \cdot p \models x \in z && \text{Lemma 5.10} \quad \square
 \end{aligned}$$

7. THE INTERNAL ALGEBRAIC THEORY OF PREPOINTS

In this technical subsection we develop the ‘internal algebra’—in the sense of ‘a theory of equalities’—of our models. We consider ways in which two internal sets can be considered equivalent (‘equal’), relative to a set of internal sets or to a prepoint.

This will help us develop the theory of points in Definition 8, starting with Definition 8.3. It will also be developed further, in Section 10.

The main definitions are just below. The main results are Propositions 7.5 and 7.6 and Corollary 7.7.

7.1. The basic definitions and lemmas

DEFINITION 7.1. Suppose $j \in \mathbb{Z}$ and $\mathcal{Y} \subseteq \text{Set}^j$. Suppose $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$. Then define $\mathcal{Y} \models u = u'$ by

$$\mathcal{Y} \models u = u' \text{ when } \forall a \in \mathbb{A}^i. \forall y \in \text{Set}^j. (y[a \mapsto u] \in \mathcal{Y} \Leftrightarrow y[a \mapsto u'] \in \mathcal{Y}).$$

We say that \mathcal{Y} **intensionally equates** u and u' .

DEFINITION 7.2. Suppose $p \in \text{PrPt}$. Suppose $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$. Then define

- $p \models u = u'$, read “ p **intensionally equates** u and u' ”, and
- $p \Vdash u = u'$, read “ p **extensionally equates** u and u' ”,

by

$$\begin{aligned}
 p \models u = u' &\text{ when } \forall a \in \mathbb{A}. (pa \models u = u') \\
 p \Vdash u = u' &\text{ when } pu = pu'.
 \end{aligned}$$

Above, pa and pu are from Definition 6.2 and $pa \models u = u'$ is from Definition 7.1.

We may write $p \models a = u'$ as shorthand for $p \models \text{atm}(a) = u'$, and similarly for $p \Vdash a = u'$.

REMARK 7.3. It may be helpful to unpack Definition 7.2 a little:

- $p \models u = u'$ when $p \models z[c \mapsto u] \in a \Leftrightarrow p \models z[c \mapsto u'] \in a$, for all z, a , and c of appropriate levels.
- $p \Vdash u = u'$ when $p \models y \in u \Leftrightarrow p \models y \in u'$ for all $y \in \text{Set}^{i-1}$.

Lemma 7.4 will be helpful for proving Proposition 7.5:

LEMMA 7.4. Suppose $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $p \in \text{PrPt}$ and $p \models u = u'$. Then

$$p \models y[a \mapsto u] \in b \Leftrightarrow p \models y[a \mapsto u'] \in b.$$

Proof. We unpack Definitions 7.1 and 7.2, and Definition 6.2. □

7.2. Equalities

PROPOSITION 7.5. *Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $p \models u = u'$ and $p \Vdash u = u'$. Then for every $a \in \mathbb{A}^i$ and $j \in \mathbb{Z}$ and $y \in \text{Set}^j$ and $x \in \text{Set}^{j+1}$ we have:*

- (1) $p \models y[a \mapsto u] \in x \Leftrightarrow p \models y[a \mapsto u'] \in x$
- (2) $p \models y \in (x[a \mapsto u]) \Leftrightarrow p \models y \in (x[a \mapsto u'])$

Proof. Fix some $k' \in \mathbb{Z}$. We prove the Lemma for all y and x such that $\text{minlevel}(y, a, x) \geq k'$ (Definition 4.4), reasoning by induction on $(\text{level}(x), \text{age}(x))$ lexicographically ordered. Since k' was arbitrary, this suffices to prove it for all y and x .

Since we work by induction on $\text{age}(x)$, it is convenient to use Notation 6.14 (int, cmp, every) in what follows:

— The case $x = \text{atm}(b)$ for $b \in \mathbb{A}^{j+1}$.

$$\begin{aligned} p \models y[a \mapsto u] \in b &\Leftrightarrow p \models y[a \mapsto u'] \in b && \text{Fig3(modelt), } p \models u = u' \\ p \models y \in b[a \mapsto u] &\Leftrightarrow p \models y \in b && \text{Figure 1}(\sigma b) \\ &\Leftrightarrow p \models y \in b[a \mapsto u'] && \text{Figure 1}(\sigma b) \end{aligned}$$

— The case $x = \text{atm}(a)$ where $i = j + 1$.

$$\begin{aligned} p \models y[a \mapsto u] \in a &\Leftrightarrow p \models y[a \mapsto u'] \in a && \text{Fig3(modelt), } p \models u = u' \\ p \models y \in a[a \mapsto u] &\Leftrightarrow p \models y \in u && \text{Figure 1}(\sigma a) \\ &\Leftrightarrow p \models y \in u' && p \models u = u' \\ &\Leftrightarrow p \models y \in a[a \mapsto u'] && \text{Figure 1}(\sigma a) \end{aligned}$$

— The case $x = [b](z \in c)$ for $b \in \mathbb{A}^j$ and $k \in \mathbb{Z}$ and $z \in \text{Set}^k$ and $c \in \mathbb{A}^{k+1}$. Using Lemma 2.64 assume $b \# u, u'$.

Also, using Lemma 4.7 we assume $a \# z$, and we reason as follows:

$$\begin{aligned} p \models y[a \mapsto u] \in [b](z \in c) &\Leftrightarrow p \models z[b \mapsto y[a \mapsto u]] \in c && \text{Lemma 6.5} \\ &\Leftrightarrow p \models z[b \mapsto y[a \mapsto u']] \in c && \text{Corollary 4.15, } a \# z, b \# u \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u] \in c && \text{Fig3(modelt), } p \models u = u' \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u'] \in c && \\ \dots &\Leftrightarrow p \models y[a \mapsto u'] \in [b](z \in c) \end{aligned}$$

Using Lemma 4.7 we assume $a \# y$, and we reason as follows:

$$\begin{aligned} p \models y \in ([b](z \in c))[a \mapsto u] &\Leftrightarrow p \models y \in [b](z[a \mapsto u] \in c) && \text{Fig1}(\sigma[]), b \# u, \text{Lem 6.6(3)} \\ &\Leftrightarrow p \models z[a \mapsto u][b \mapsto y] \in c && \text{Lemma 6.5} \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u] \in c && \text{Corollary 4.14, } a \# y, b \# u \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u'] \in c && \text{Fig3(modelt), } p \models u = u' \\ \dots &\Leftrightarrow p \models y \in ([b](z \in c))[a \mapsto u'] \end{aligned}$$

— The case $x = [b](z \in b)$ for $b \in \mathbb{A}^j$ and $z \in \text{Set}^{j-1}$. Using Lemma 2.64 assume $b \# u, u'$.

Also, using Lemma 4.7 we assume $a \# z$, and we reason as follows:

$$\begin{aligned} p \models y[a \mapsto u] \in [b](z \in b) &\Leftrightarrow p \models z[b \mapsto y[a \mapsto u]] \in y[a \mapsto u] && \text{Lemma 6.5} \\ &\Leftrightarrow p \models z[b \mapsto y[a \mapsto u']] \in y[a \mapsto u'] && \text{IH(2) } \text{level}(y) < \text{level}(x) \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u] \in y[a \mapsto u'] && \text{Corollary 4.15, } a \# z, b \# u \\ &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u'] \in y[a \mapsto u'] && \text{IH(1) } \text{level}(y[a \mapsto u']) < \text{level}(x) \\ \dots &\Leftrightarrow p \models y[a \mapsto u'] \in [b](z \in b) \end{aligned}$$

Using Lemma 4.7 we assume $a\#y$, and we reason as follows:

$$\begin{aligned}
 p \models y \in ([b](z \in b))[a \mapsto u] &\Leftrightarrow p \models y \in [b](z[a \mapsto u] \in b) && \text{Fig 1}(\sigma[]), b\#u, \text{Lem 6.6(3)} \\
 &\Leftrightarrow p \models z[a \mapsto u][b \mapsto y] \in y && \text{Lemma 6.5} \\
 &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u] \in y && \text{Corollary 4.14, } a\#y, b\#u \\
 &\Leftrightarrow p \models z[b \mapsto y][a \mapsto u'] \in y && \text{IH(1) } level(y) < level(x) \\
 \dots &\Leftrightarrow p \models y[a \mapsto u] \in ([b](z \in b))[a \mapsto u']
 \end{aligned}$$

— The case $x = \text{int}(x)$ for $x \subseteq_{\text{fin}} \text{Set}^{j+1}$ a finite set of internal comprehensions.

We reason as follows:

$$\begin{aligned}
 p \models y[a \mapsto u] \in \text{int}(x) &\Leftrightarrow \forall x' \in x. p \models y[a \mapsto u] \in x' && \text{Proposition 6.17(1)} \\
 &\Leftrightarrow \forall x' \in x. p \models y[a \mapsto u'] \in x' && \text{IH(1) } age(x') < age(\text{int}(x)) \\
 &\Leftrightarrow p \models y[a \mapsto u'] \in \text{int}(x) && \text{Proposition 6.17(1)} \\
 p \models y \in (\text{int}(x)[a \mapsto u]) &\Leftrightarrow p \models y \in \text{int}(\{x'[a \mapsto u] \mid x' \in x\}) && \text{Lemma 6.16(1)} \\
 &\Leftrightarrow \forall x' \in x. p \models y \in (x'[a \mapsto u]) && \text{Proposition 6.17(1)} \\
 &\Leftrightarrow \forall x' \in x. p \models y \in (x'[a \mapsto u']) && \text{IH(2) } age(x') < age(\text{int}(x)) \\
 \dots &\Leftrightarrow p \models y \in ([b]\text{int}(x))[a \mapsto u']
 \end{aligned}$$

— The case $x = \text{cmp}(x')$ for $x' \in \text{Set}^{j+1}$.

We reason as follows:

$$\begin{aligned}
 p \models y[a \mapsto u] \in \text{cmp}(x') &\Leftrightarrow p \not\models y[a \mapsto u] \in x' && \text{Proposition 6.17(2)} \\
 &\Leftrightarrow p \not\models y[a \mapsto u'] \in x' && \text{IH(1) } age(x') < age(\text{cmp}(x')) \\
 &\Leftrightarrow p \models y[a \mapsto u'] \in \text{cmp}(x') && \text{Proposition 6.17(2)} \\
 p \models y \in (\text{cmp}(x')[a \mapsto u]) &\Leftrightarrow p \models y \in \text{cmp}(x'[a \mapsto u]) && \text{Lemma 6.16(1)} \\
 &\Leftrightarrow p \not\models y \in x'[a \mapsto u] && \text{Proposition 6.17(2)} \\
 &\Leftrightarrow p \not\models y \in x'[a \mapsto u'] && \text{IH(2) } age(x') < age(\text{cmp}(x')) \\
 &\Leftrightarrow p \models y \in \text{cmp}(x'[a \mapsto u']) && \text{Proposition 6.17(2)}
 \end{aligned}$$

— The case $x = \text{every}[a']x'$ for $x' \in \text{Set}^{j+1}$ and $i' \in \mathbb{Z}$ and $a' \in \mathbb{A}^{i'}$.

Using Lemma 4.7 we assume $a'\#u, u', y$, and we reason as follows:

$$\begin{aligned}
 p \models y[a \mapsto u] \in \text{every}[a']x' &\Leftrightarrow \forall a'' \in \mathbb{A}^{i'}. (a'' a') \cdot p \models y[a \mapsto u] \in x' && \text{Proposition 6.17(3), } a'\#y \\
 &\Leftrightarrow \forall a'' \in \mathbb{A}^{i'}. (a'' a') \cdot p \models y[a \mapsto u'] \in x' && \text{IH(1) } age(x') < age(\text{every}[a']x') \\
 \dots &\Leftrightarrow p \models y[a \mapsto u'] \in \text{every}[a']x' \\
 p \models y \in (\text{every}[a']x'[a \mapsto u]) &\Leftrightarrow p \models y \in \text{every}[a'](x'[a \mapsto u]) && \text{Lemma 6.16(3), } a'\#u \\
 &\Leftrightarrow \forall a'' \in \mathbb{A}^{i'}. (a'' a') \cdot p \models y \in x'[a \mapsto u] && \text{Proposition 6.17(3), } a'\#y \\
 &\Leftrightarrow \forall a'' \in \mathbb{A}^{i'}. (a'' a') \cdot p \models y \in x'[a \mapsto u'] && \text{IH(2) } age(x') < age(\text{every}[a']x') \\
 \dots &\Leftrightarrow p \models y \in (\text{every}[a']x')[a \mapsto u']
 \end{aligned}$$

□

PROPOSITION 7.6. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $X \in \text{Pred}$. Then

$$p \models u = u' \wedge p \Vdash u = u' \text{ implies } p \models X[a \mapsto u] \Leftrightarrow p \models X[a \mapsto u'].$$

Proof. With what we have proved so far, this is by a routine induction on X . We consider the possibilities for X :

— The case $X = z \in a'$ where $i' \in \mathbb{Z}$ and $a' \in \mathbb{A}^{i'}$ and $z \in \text{Set}^{i'-1}$. We reason as follows:

$$\begin{aligned}
 p \models (z \in a')[a \mapsto u] &\Leftrightarrow p \models z[a \mapsto u] \in a' && \text{Lemma 6.6(3)} \\
 &\Leftrightarrow p \models z[a \mapsto u'] \in a' && \text{Lemma 7.4, } p \models u = u' \\
 &\Leftrightarrow p \models (z \in a')[a \mapsto u'] && \text{Lemma 6.6(3)}
 \end{aligned}$$

— The case $X = z \in a$ where $z \in \text{Set}^{i-1}$. We reason as follows:

$$\begin{aligned}
 p \models (z \in a)[a \mapsto u] &\Leftrightarrow p \models z[a \mapsto u] \in u && \text{Lemma 6.6(2)} \\
 &\Leftrightarrow p \models z[a \mapsto u] \in u' && p \Vdash u = u' \\
 &\Leftrightarrow p \models z[a \mapsto u'] \in u' && \text{Proposition 7.5, } p \models u = u', p \Vdash u = u' \\
 &\Leftrightarrow p \models (z \in a)[a \mapsto u'] && \text{Lemma 6.6(2)}
 \end{aligned}$$

— The case $X = \text{and}(\mathcal{X})$ where $\mathcal{X} \subseteq_{\text{fin}} \text{Pred}$. We reason as follows:

$$\begin{aligned}
 p \models \text{and}(\mathcal{X})[a \mapsto u] &\Leftrightarrow p \models \text{and}(\{X'[a \mapsto u] \mid X' \in \mathcal{X}\}) && \text{Figure 1}(\sigma\text{and}) \\
 &\Leftrightarrow \forall X' \in \mathcal{X}. p \models X'[a \mapsto u] && \text{Figure 3(modand)} \\
 &\Leftrightarrow \forall X' \in \mathcal{X}. p \models X'[a \mapsto u'] && \text{IH } \text{age}(X') < \text{age}(\text{and}(\mathcal{X})) \\
 \dots &\Leftrightarrow p \models \text{and}(\mathcal{X})[a \mapsto u']
 \end{aligned}$$

— The case $X = \text{neg}(X')$ where $X' \in \text{Pred}$. We reason as follows:

$$\begin{aligned}
 p \models \text{neg}(X')[a \mapsto u] &\Leftrightarrow p \models \text{neg}(X'[a \mapsto u]) && \text{Figure 1}(\sigma\text{neg}) \\
 &\Leftrightarrow p \not\models X'[a \mapsto u] && \text{Figure 3(modneg)} \\
 &\Leftrightarrow p \not\models X'[a \mapsto u'] && \text{IH } \text{age}(X') < \text{age}(\text{neg}(X')) \\
 \dots &\Leftrightarrow p \models \text{neg}(X')[a \mapsto u']
 \end{aligned}$$

— The case $X = \text{all}[b]X'$ where $j \in \mathbb{Z}$ and $b \in \mathbb{A}^j$ and we assume using Lemma 2.64 that $b \# u, u'$. We reason as follows:

$$\begin{aligned}
 p \models (\text{all}[b]X')[a \mapsto u] &\Leftrightarrow p \models \text{all}[b](X'[a \mapsto u]) && \text{Figure 1}(\sigma\text{all}) \ b \# u \\
 &\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' \ b) \cdot p \models X'[a \mapsto u] && \text{Lemma 5.10} \\
 &\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' \ b) \cdot p \models X'[a \mapsto u'] && \text{IH } \text{age}(X') < \text{age}(\text{all}[b]X') \\
 \dots &\Leftrightarrow p \models (\text{all}[b]X')[a \mapsto u']
 \end{aligned}$$

□

We use Corollary 7.7 later in Lemma 12.50; we mention it now since it belongs to the same family of results as Proposition 7.6:

COROLLARY 7.7. *Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$. Then the following conditions are equivalent:*

$$p \models u = u' \wedge p \Vdash u = u' \quad \Leftrightarrow \quad \forall z \in \text{Set}^{i+1}. (p \models u \in z \Leftrightarrow p \models u' \in z).$$

Proof. The left-to-right implication follows by routine calculations combining Proposition 7.6 with Lemmas 6.6(1) and 4.9.

We now consider the right-to-left implication. Suppose $\forall z \in \text{Set}^{i+1}. (p \models u \in z \Leftrightarrow p \models u' \in z)$.

- If we consider all z of the form $z = [c](y \in c)$ for $y \in \text{Set}^{i-1}$ and $c \in \mathbb{A}^i$ and $c \# y$, then we deduce using Corollary 6.7 that $p \models y \in u \Leftrightarrow p \models y \in u'$ and so by Definition 7.2 that $p \Vdash u = u'$.
- If we consider all z of the form $[c](z' \in a')$ for $i' \in \mathbb{Z}$ and $a' \in \mathbb{A}^{i'}$ and $c \in \mathbb{A}^i$ then we deduce using Lemmas 6.5 and 6.6(3) that $p \Vdash u = u'$. □

REMARK 7.8. Proposition 7.6 and Corollary 7.7 are representatives of a family of similar results. It might be useful to mention them. It is a fact that the following are all equivalent, where $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$:

- $p \models u = u' \wedge p \Vdash u = u'$.
- $\forall z \in \text{Set}^{i+1}. (p \models u \in z \Leftrightarrow p \models u' \in z)$.
- $\forall Z \in \text{Pred}. \forall a \in \mathbb{A}^i. (p \models Z[a \mapsto u] \Leftrightarrow p \models Z[a \mapsto u'])$. (Proposition 7.6 handles one direction.)
- $\forall c \in \mathbb{A}^i. p[u \leftarrow c] = p[u' \leftarrow c]$ (easily proved from the above using Theorem 5.17 and Lemma 5.11).
- $\forall z \in \text{Set}^{i+1}. pz \models u = u'$.

8. POINTS

In this Section we discuss *points* and their abstract properties. The main definition is Definition 8.3. Points are ‘nice’ prepoints with useful extra properties over prepoints; see notably Theorems 8.15 and 8.20.

In Section 9 we show that NF is consistent provided that points exist (in fact we consider an equivalent system TST+). See Corollary 9.30. Then, the rest of this paper is devoted to actually constructing a point, culminating with Corollary 12.51 and Theorem 12.52.

8.1. The basic definition

DEFINITION 8.1. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $x \in \text{Set}^i$. Say that p **generously names** x when for every $a \in \mathbb{A}^i$ and $X \in \text{Pred}$,

$$\exists a' \in \mathbb{A}^i. (p \models (a' a) \cdot X \Leftrightarrow p \models X[a \mapsto x]).$$

Unpacking Definition 2.34, this means $p \models (a' a) \cdot X \Leftrightarrow p \models X[a \mapsto x]$ for generously many $a' \in \mathbb{A}^i$.

REMARK 8.2. A few words of intuition for Definition 8.1. Recall from Figure 3 (**modall**) that $p \models \text{all}[a]X$ when $\forall a'. p \models (a' a) \cdot X$, or in words: \forall is translated to \mathbb{A} . Thus \exists (the dual of \forall) is translated to \mathbb{D} (the dual of \mathbb{A}).

So p generously names x when $p \models \text{exists}[a](X \Leftrightarrow (X[a \mapsto x]))$ (where $\text{exists}[a]Z$ is sugar for $\text{neg}(\text{all}[a]\text{neg}(Z))$, as we would expect), or in more familiar notation: $\exists a. (X \Leftrightarrow X[a \mapsto x])$.

Note that the generous set of atoms witnessing this existential may vary not only with p and x , but also with X .

DEFINITION 8.3. Suppose $p \in \text{PrPt}$.

- (1) Say $p \in \text{PrPt}$ **generously names internal sets** when p generously names x for every $x \in \text{Set}$. (See also Definitions 11.29 and 11.35.)
- (2) Call $p \in \text{PrPt}$ **extensional** when for every $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$

$$p \Vdash x = x' \Rightarrow p \models x = x'.$$

\Vdash and \models are from Definition 7.2.

- (3) Following Notation 2.22, we call $p \in \text{PrPt}$ **ϑ -ambiguous** when

$$p = \vartheta \cdot p$$

for some shift permutation ϑ (Definition 2.13), and **ambiguous** when it is ϑ -ambiguous for some ϑ .

Recall from Definition 2.29 that $\vartheta \cdot p = \{\vartheta(a) \circ \vartheta \cdot x \mid a \circ x \in p\}$.

- (4) Call $p \in \text{PrPt}$ a **point** when
 - (i) it is extensional,
 - (ii) it is ambiguous, and
 - (iii) it generously names every internal set.

Write Pnt for the set of prepoints that are points, thus:

$$\text{Pnt} = \{p \in \text{PrPt} \mid p \text{ is a point}\}.$$

REMARK 8.4. For the reader’s convenience we list where the clauses of Definition 8.3 are used:

- (1) We use clause 1 in Lemma 8.14.
- (2) We use clause 2 in Theorem 8.20.
- (3) We use clause 3 in Theorem 9.28.

LEMMA 8.5. $\text{supp}(\text{Pnt}) = \emptyset$, so Pnt is equivariant (Definition 2.44) and $a \# \text{Pnt}$ for any atom a .

Proof. Direct from Theorem 2.31. The corollaries just rephrase the result using Definition 2.44 and Notation 2.26. \square

Recall $p \models X$ from Figure 3. We may use Notation 8.6 henceforth:

NOTATION 8.6. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $x \in \text{Set}^i$ and $p \in \text{Pnt}$ and $a \in \mathbb{A}^i$. Then we may write:

$$\begin{aligned} \llbracket X \rrbracket & \text{ for } \{p \in \text{Pnts} \mid p \models X\} \text{ and} \\ \llbracket x \rrbracket & \text{ for } \llbracket x \rrbracket^{\text{Pnt}}. \end{aligned}$$

$\llbracket x \rrbracket^{\text{Pnt}}$ is from Definition 5.4(2).

8.2. Quantification

REMARK 8.7. We consider properties of the denotation $\llbracket \text{all}[a]X \rrbracket$ of $\text{all}[a]X$ over points. For the reader's convenience we sum them up here:

- Lemma 8.9 rephrases Figure 3 (**modall**) using \mathcal{U} from Definition 2.54.
- Lemma 8.11 states that if $a \# \llbracket X \rrbracket$ then $\llbracket \text{all}[a]X \rrbracket = \llbracket X \rrbracket$. This corresponds to “if a is fresh for ϕ then $\forall a. \phi \Leftrightarrow \phi$ ”.
- Lemma 8.12 implies soundness of (**allR**) in Figure 6 (see Lemma 9.16). We can think of this as corresponding to the right-intro rule (**VR**) for universal quantification.
- Lemma 8.14 states that $\llbracket \text{all}[a]X \rrbracket \subseteq \llbracket X[a \mapsto x] \rrbracket$ (also $\llbracket \text{all}[a]X \rrbracket \subseteq \llbracket X \rrbracket$). This implies soundness of (**instantiation**) in Figure 6 (see Lemma 9.16).
- Theorem 8.15 corresponds to the intuition that $\forall a. \phi$ should be equal to an infinite conjunction of $\phi[a \mapsto x]$ for all possible x .
- Lemma 8.16 states that all is monotone. Intuitively, this corresponds to “ $\phi \Rightarrow \psi$ implies $\forall a. \phi \Rightarrow \forall a. \psi$ ”.

REMARK 8.8. The results in this Subsection fall into two groups:

Lemmas 8.9, 8.11, 8.12, and 8.16 are proved using general properties of permutations and of \mathcal{U} from Definition 2.54. The proofs are general, and fairly simple.

Lemma 8.14 and Theorem 8.15 use specific properties of points from Definition 8.3; their proofs are (slightly) harder but moreover they depend on the fact that $\llbracket X \rrbracket$ uses sets of *points* rather than just prepoints. See Remark 8.4.

LEMMA 8.9. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$\llbracket \text{all}[a]X \rrbracket = \mathcal{U}a. \llbracket X \rrbracket.$$

Proof. From Lemmas 5.10 and 2.56. □

REMARK 8.10. Lemma 8.9 is very easy to prove but it brings out something that was only implicit until now: the sets interpretation of quantification.

The reader will be unsurprised that conjunction is modelled by intersection and negation by complement. Because of our use of nominal sets, quantification also corresponds to an abstract sets operation—by ‘abstract’, we mean one that is defined (like sets intersection and complement) for arbitrary sets.¹⁵ This sets operation is the \mathcal{U} -quantifier on nominal sets, which exists for any nominal set and thus is ‘abstract’ in the sense just discussed.

Thus we have:

$$\llbracket \text{and}\{X_1, \dots, X_n\} \rrbracket = \bigcap_j \llbracket X_j \rrbracket \quad \llbracket \text{neg}(X) \rrbracket = \text{Pnt} \setminus \llbracket X \rrbracket \quad \llbracket \text{all}[a]X \rrbracket = \mathcal{U}a. \llbracket X \rrbracket.$$

The two left-hand equalities are standard; the right-hand one is characteristic of ideas inherited from [Gab16; GG16], thus, of the general approach to names and binding in semantics on which this paper is based.

LEMMA 8.11. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then:

¹⁵So an operation that depends on acting on a set of valuations does not count here as ‘abstract’.

- (1) If $a\# [X]$ then $[a11[a]X] = [X]$.
 (2) If $[X] = \text{Pnt}$ then $[a11[a]X] = \text{Pnt}$.

Proof. We reason as follows:

$$\begin{aligned} [a11[a]X] &= \mathcal{U}a. [X] && \text{Lemma 8.9} \\ &= [X] && \text{Lemma 2.59, } a\#[X] \end{aligned}$$

For part 2, if $[X] = \text{Pnt}$ then by Lemma 8.5 $a\#[X]$ and by part 1 of this result $[a11[a]X] = [X]$. \square

LEMMA 8.12. Suppose $X, Y \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $a\#X$. Then

$$[a11[a]\text{imp}(X, Y)] = [\text{imp}(X, a11[a]Y)].$$

Proof. We unpack Notation 3.8 and use the rules of Figure 3 and Lemma 2.61(4). By Theorem 2.31(3) $a\#(\text{Pnt} \setminus [X])$, because $a\#X$. \square

REMARK 8.13. It is not in general the case that $p \models a11[a]X$ implies $p \models X[a \mapsto x]$. However, we shall note while proving Lemma 8.14 that if p generously names internal sets then $p \models (a' a) \cdot X$ for fresh a' implies that $p \models (a' a) \cdot X$ for some a' naming x ; and this is enough.

LEMMA 8.14. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then:

- (1) $[a11[a]X] \subseteq [X[a \mapsto x]]$.
 (2) $[a11[a]X] \subseteq [X]$.

Proof. Suppose $p \in \text{Pnt}$ and $p \models a11[a]X$, so that by Lemma 5.10 $\mathcal{U}a' \in \mathbb{A}^i. (p \models (a' a) \cdot X)$. By clause 1 of Definition 8.3 $\exists a' \in \mathbb{A}^i. (p \models (a' a) \cdot X \Leftrightarrow p \models X[a \mapsto x])$.

Using Lemma 2.11(5) there exists an $a' \in \mathbb{A}^i$ such that $p \models (a' a) \cdot X$ and also $p \models (a' a) \cdot X \Leftrightarrow p \models X[a \mapsto x]$, so that $p \models X[a \mapsto x]$ as required.

Part 2 follows using part 1 and Lemma 4.16. \square

We now come to Theorem 8.15, which proves that on sets of points, universal quantification does indeed coincide with intersection over all internal sets. Recall from Notation 8.6 that Theorem 8.15 works over *points*—so compare this with Lemma 5.10 which is all we could prove over *prepoints*:

THEOREM 8.15. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $X \in \text{Pred}$. Then

$$[a11[a]X] = \bigcap_{x \in \text{Set}^i} [X[a \mapsto x]].$$

Proof. The left-to-right subset inclusion is from Lemma 8.14.

For the right-to-left subset inclusion, by Figure 3 (**moda11**) it suffices to show of $p \in \text{Pnt}$ that $\forall x \in \text{Set}^i. p \models X[a \mapsto x]$ implies $\mathcal{U}a' \in \mathbb{A}^i. p \models (a' a) \cdot X$. This follows using Lemma 4.17(1), taking any $a' \# X$. \square

We never use Lemma 8.16 but we mention it anyway because it nicely illustrates how Lemma 8.9 is used:

LEMMA 8.16. Suppose $X, X' \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then

$$\begin{aligned} [X] \subseteq [X'] &\text{ implies } [a11[a]X] \subseteq [a11[a]X'] \text{ and} \\ [X] = [X'] &\text{ implies } [a11[a]X] = [a11[a]X']. \end{aligned}$$

Proof. Suppose $[X] \subseteq [X']$. We reason as follows:

$$\begin{aligned} [a11[a]X] &= \mathcal{U}a. [X] && \text{Lemma 8.9} \\ &\subseteq \mathcal{U}a. [X'] && \text{Lemma 2.60, } [X] \subseteq [X'] \\ &= [a11[a]X'] && \text{Lemma 8.9} \end{aligned}$$

The second part follows by facts of sets. \square

$$\begin{array}{l} \phi, \psi ::= \perp \mid \phi \Rightarrow \phi \mid \forall a. \phi \mid s = s \mid s \in s \\ s, t ::= a \mid \{a \mid \phi\} \end{array}$$

Fig. 5: Formulae and terms of TST/TST+

8.3. Extensionality

The main result of this Subsection is Theorem 8.20. Intuitively this asserts that if a point p believes that x and x' have the same elements, then p believes that no Z can distinguish them. Thus inside the model, extensional equality implies indistinguishability (Leibniz equality). This leads to soundness of (**Leibniz**) from Figure 6 in Theorem 9.18.

REMARK 8.17. The denotation over prepoints is intensional, in the sense that if $p \in \text{PrPt}$ then $px = px'$ does not in general imply $p \models x \in z \Leftrightarrow x' \in z$.

Take for instance $x = \text{elt}(\text{empt}^{i-1}, a)$ and $x' = \text{elt}(\text{int}(\{\text{empt}^{i-1}, \text{empt}^{i-1}\}), a)$ for some $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. Then it is a fact that there exists a prepoint p and an atom a such that $px = px'$ and $p \not\models x \in a \Leftrightarrow x' \in a$.

For Pnt the implication does hold and we call the denotation $\llbracket - \rrbracket^{\text{Pnt}}$ **extensional**.

Some notation will help readability:

NOTATION 8.18.— If $X, Y \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ define $X \Rightarrow Y$ and $X \Leftrightarrow Y$ and $\forall a. X$ extending Notation 3.8 by:

$$\begin{aligned} X \Rightarrow Y &= \text{imp}(X, Y) \\ X \Leftrightarrow Y &= \text{iff}(X, Y) \\ \forall a. X &= \text{all}[a]X \end{aligned}$$

— If $i \in \mathbb{Z}$ and $x, y \in \text{Set}^i$ then define $x = y$ by:

$$x = y = \forall c. (c \in x \Leftrightarrow c \in y)$$

Above, we take $c \in \mathbb{A}^{i-1}$ fresh (so $c \# x, y$).

LEMMA 8.19. Suppose $p \in \text{Pnt}$ and $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$. Then if $p \models x = x'$ then $p \models x = x'$.

Proof. Suppose $p \models x = x'$. We unpack Notation 8.18 and use Theorem 8.15 and conclude that

$$\forall y \in \text{Set}^{i-1}. p \models y \in x \Leftrightarrow p \models y \in x'.$$

By Definition 6.2 $p(x) = p(x')$ as required. □

Theorem 8.20 expresses soundness of (**Leibniz**) in Figure 6 (see Theorem 9.18):

THEOREM 8.20. Suppose $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$ and $a \in \mathbb{A}^i$. Then (using Notation 8.18)

$$\llbracket x = x' \rrbracket \subseteq \llbracket Z[a \mapsto x] \Leftrightarrow Z[a \mapsto x'] \rrbracket.$$

Proof. Suppose $p \in \text{Pnt}$ and $p \models x = x'$. By Lemma 8.19 $p \models x = x'$ and by clause 2 of Definition 8.3 $p \models x = x'$. Therefore by Proposition 7.6 and Lemma 5.9(2) $p \models Z[a \mapsto x] \Leftrightarrow Z[a \mapsto x']$. □

9. TYPED SET THEORY

9.1. Formulae of the language of typed set theory

DEFINITION 9.1. Let **formulae** and **terms** be inductively defined as in Figure 5. In that figure, a ranges over atoms of level at least 1.

Definition 9.2 is standard:

DEFINITION 9.2. Suppose t is a term (Definition 9.1). Then extend $\text{level}(a)$ from Definition 2.4 from atoms to all terms by:

$$\text{level}(\{a \mid \phi\}) = \text{level}(a) + 1$$

Call a formula ϕ or term t **stratified** when:

(modus ponens)	If $\vdash \phi$ and $\vdash \phi \Rightarrow \psi$ then $\vdash \psi$	
(generalisation)	If $\vdash \phi$ then $\vdash \forall a. \phi$	
(K)	$\vdash \phi \Rightarrow (\psi \Rightarrow \phi)$	
(S)	$\vdash ((\phi \Rightarrow \psi) \Rightarrow \xi) \Rightarrow (\phi \Rightarrow \psi) \Rightarrow (\phi \Rightarrow \xi)$	
(contrapositive)	$\vdash (\neg \psi \Rightarrow \neg \phi) \Rightarrow (\phi \Rightarrow \psi)$	
(instantiation)	$\vdash (\forall a. \phi) \Rightarrow (\phi[a:=s])$	
(allR)	$\vdash (\forall a. (\phi \Rightarrow \psi)) \Rightarrow (\phi \Rightarrow \forall a. \psi)$	a not free in ϕ
(identity)	$\vdash s=s$	
(Leibniz)	$\vdash s=t \Rightarrow (\phi[a:=s] \Leftrightarrow \phi[a:=t])$	
(extensionality)	$\vdash (s=t) \Leftrightarrow \forall c. (c \in s \Leftrightarrow c \in t)$	c not free in s, t
(comprehension)	$\vdash s \in \{a \mid \phi\} \Leftrightarrow \phi[a:=s]$	

Fig. 6: Axioms of TST

(TA)	$\vdash \phi \Rightarrow \phi^+$
------	----------------------------------

Fig. 7: Additional *typical ambiguity* axiom of TST+

- If $s' \in s$ is a subterm of t or ϕ then $\text{level}(s) = \text{level}(s') + 1$.
- If $s' = s$ is a subterm of t or ϕ then $\text{level}(s) = \text{level}(s')$.

EXAMPLE 9.3. Suppose $a \in \mathbb{A}^2$, $b \in \mathbb{A}^3$, and $c \in \mathbb{A}^4$. Then $a \in b$, $b \in c$, and $a = a$ are stratified, and $a \in c$, $b \in a$, $a \in a$, and $a = b$ are not stratified.

DEFINITION 9.4. The language of **typed set theory (TST)** consists of stratified formulae and terms. A Hilbert-style derivation system for TST is given in Figure 6.

In that figure and henceforth, we write $\phi[a:=s]$ and $t[a:=s]$ for the usual capture-avoiding substitution on syntax.

We assume that levels are arranged to respect stratification, so that when we write $[a:=s]$ it is understood that we assume $a \in \mathbb{A}^{\text{level}(s)}$.

REMARK 9.5. We only care about *stratified* formulae and terms henceforth—that is, we restrict attention from all (raw) formulae and terms of Definition 9.1, to those that are stratified.

So for all terms and formulae considered from now on, the reader should assume they are stratified.

REMARK 9.6. In Definition 3.1 levels ranged over all of \mathbb{Z} . In TST types/levels range over strictly positive natural numbers 1, 2, 3, 4, ... and (continuing in the language of types)

- \in polymorphically takes two terms of type i and $i+1$ to a formula for each $i \geq 1$,
- equality polymorphically takes two terms of type i to a formula, and
- sets comprehension $\{a \mid \phi\}$ takes an atom of type $i \geq 1$ and a formula ϕ to a term of type $i+1$.

9.2. Interpretation for formulae and terms

DEFINITION 9.7. Define an **interpretation** of stratified formulae ϕ and terms s as in Figure 8, mapping ϕ to $\langle \phi \rangle \in \text{Pred}$ and s of level $i \geq 1$ to $\langle s \rangle \in \text{Set}^i$.

REMARK 9.8. For the reader's convenience we give pointers for the notation used in the right-hand sides of the equalities in Figure 8:

- `false` is from Example 3.9.
- `neg` is from Definition 3.1.
- `imp` and `iff` are from Notation 3.8.
- $\langle s \rangle = \langle t \rangle$ is from Notation 8.18.

$\langle \perp \rangle = \text{false}$	$\langle s=t \rangle = \langle s \rangle = \langle t \rangle$
$\langle \phi \Rightarrow \psi \rangle = \text{imp}(\langle \phi \rangle, \langle \psi \rangle)$	$\langle t \in s \rangle = \langle t \rangle \in \langle s \rangle$
$\langle \forall a. \phi \rangle = \text{all}[a] \langle \phi \rangle$	$\langle \{a \phi\} \rangle = [a] \langle \phi \rangle$
	$\langle a \rangle = \text{atm}(a)$

Fig. 8: Interpretation of formulae and terms

- $\langle t \rangle \in \langle s \rangle$ is from Notation 6.1.
- $[a] \langle \phi \rangle$ is from Definitions 2.62 and 3.1.
- atm is from Definition 3.1.

REMARK 9.9. Figure 8 translates the syntax of formulae ϕ and terms s from Figure 5 to the syntax of internal predicates and internal sets from Definition 3.1. This translation is not entirely direct:

- (1) $s=t$ is translated to a universally quantified extensional equality; see Notation 8.18.
- (2) $t \in s$ is primitive in formulae but only primitive in internal predicates if s is an atom.

LEMMA 9.10. *Suppose ϕ is a stratified formula and s is a stratified term, and suppose $\text{level}(s)=i$. Then*

$$\langle \phi \rangle \in \text{Pred} \quad \text{and} \quad \langle s \rangle \in \text{Set}^i.$$

Proof. By induction on ϕ and s :

- *The case of a .* By Figure 8 $\langle a \rangle = \text{atm}(a)$. By Definition 3.1 $\text{atm}(a) \in \text{Set}^i$.
- *The case of $\{b | \phi\}$ for $j \geq 1$ and $b \in \mathbb{A}^j$.* By Figure 8 $\langle \{b | \phi\} \rangle = [b] \langle \phi \rangle$. By Definition 9.2 $\text{level}\{b | \phi\} = j+1$. By inductive hypothesis $\langle \phi \rangle \in \text{Pred}$ and by Definition 3.1 $[b] \langle \phi \rangle \in \text{Set}^{j+1}$.
- *The case of \perp .* By Figure 8 $\langle \perp \rangle = \text{false} \in \text{Pred}$.
- *The case of $\phi \Rightarrow \psi$.* From Figure 8 and Definition 3.1 using the inductive hypothesis.
- *The case of $\forall a. \phi$.* From Figure 8 and Definition 3.1 using the inductive hypothesis.
- *The case of $s=t$.* We refer to Notation 3.8 and use Lemma 3.10 and Figure 8 and Definition 3.1 and the inductive hypothesis.
- *The case of $t \in s$.* We refer to Notation 6.1 and use Lemma 3.10 and Proposition 4.6. □

9.3. Properties of the interpretation

DEFINITION 9.11. Define the **size** of a stratified formula ϕ and stratified term t inductively as follows:

$$\begin{aligned}
 \text{size}(a) &= 1 & \text{size}(\{a | \phi\}) &= \text{size}(\phi) + 1 \\
 \text{size}(\perp) &= 1 & \text{size}(\phi \wedge \psi) &= \text{size}(\phi) + \text{size}(\psi) + 1 \\
 \text{size}(\neg \phi) &= \text{size}(\phi) + 1 & \text{size}(\forall a. \phi) &= \text{size}(\phi) + 1 \\
 \text{size}(t \in s) &= \text{size}(t) + \text{size}(s) + 1 & \text{size}(s=t) &= \text{size}(s) + \text{size}(t) + 1
 \end{aligned}$$

LEMMA 9.12. *Suppose ϕ is a stratified formula and t , and r are stratified terms and $b \in \mathbb{A}^{\text{level}(t)}$. Then:*

$$\begin{aligned}
 \langle \phi \rangle [b \mapsto \langle t \rangle] &= \langle \phi [b := t] \rangle \\
 \langle r \rangle [b \mapsto \langle t \rangle] &= \langle r [b := t] \rangle
 \end{aligned}$$

Note by Lemma 9.10 that $\langle t \rangle \in \text{Set}^{\text{level}(t)}$ so that the σ -action $[b \mapsto \langle t \rangle]$ above is well-defined (Definition 4.1).

Proof. By induction on $\text{size}(\phi)$ and $\text{size}(r)$. We consider each case in turn:

— *The case of \perp .* We reason as follows:

$$\begin{aligned}\langle \perp \rangle[b \mapsto \langle t \rangle] &= \text{false}[b \mapsto \langle t \rangle] && \text{Figure 8} \\ &= \text{false} && \text{Corollary 4.10} \\ \langle \perp[b:=t] \rangle &= \langle \perp \rangle && \text{Fact of syntax} \\ &= \text{false} && \text{Figure 8}\end{aligned}$$

— *The case of $\phi \Rightarrow \psi$.* We reason as follows:

$$\begin{aligned}\langle \phi \Rightarrow \psi \rangle[b \mapsto \langle t \rangle] &= \text{imp}(\langle \phi \rangle, \langle \psi \rangle)[b \mapsto \langle t \rangle] && \text{Figure 8} \\ &= \text{imp}(\langle \phi \rangle[b \mapsto \langle t \rangle], \langle \psi \rangle[b \mapsto \langle t \rangle]) && \text{Figure 1 \& Notation 3.8} \\ &= \text{imp}(\langle \phi[b:=t] \rangle, \langle \psi[b:=t] \rangle) && \text{IH } \text{size}(\phi), \text{size}(\psi) < \text{size}(\phi \Rightarrow \psi) \\ &= \langle \phi[b:=t] \Rightarrow \psi[b:=t] \rangle && \text{Figure 1 \& Notation 3.8} \\ &= \langle (\phi \Rightarrow \psi)[b:=t] \rangle && \text{Fact of syntax}\end{aligned}$$

— *The case of $\forall a.\phi$.* We reason as follows, where we α -rename if necessary to assume $a \# t$ (from which it follows by Theorem 2.31 that $a \# \langle t \rangle$):

$$\begin{aligned}\langle \forall a.\phi \rangle[b \mapsto \langle t \rangle] &= (\text{all}[a](\langle \phi \rangle)[b \mapsto \langle t \rangle]) && \text{Figure 8} \\ &= \text{all}[a](\langle \phi \rangle[b \mapsto \langle t \rangle]) && \text{Figure 1 } a \# \langle t \rangle \\ &= \text{all}[a](\langle \phi[b:=t] \rangle) && \text{IH } \text{size}(\phi) < \text{size}(\forall a.\phi) \\ &= \langle \forall a.(\phi[b:=t]) \rangle && \text{Figure 8} \\ &= \langle (\forall a.\phi)[b:=t] \rangle && \text{Fact of syntax, } a \# t\end{aligned}$$

— *The case of $s=s'$.* Choose $c \in \mathbb{A}^{\text{level}(s)-1}$ fresh (so $c \# s, s', t$, so by Theorem 2.31 also $c \# \langle s \rangle, \langle s' \rangle, \langle t \rangle$). We reason as follows:

$$\begin{aligned}\langle s=s' \rangle[b \mapsto \langle t \rangle] &= (\text{all}[c](\text{iff}(\langle s \rangle @ c, \langle s' \rangle @ c))[b \mapsto \langle t \rangle]) && \text{Not 8.18, Fig 8} \\ &= \text{all}[c](\langle \langle s \rangle @ c \rangle[b \mapsto \langle t \rangle] \Leftrightarrow \langle \langle s' \rangle @ c \rangle[b \mapsto \langle t \rangle]) && \text{Not 3.8, Fig 1 } c \# \langle t \rangle \\ &= \text{all}[c](\langle \langle s \rangle[b \mapsto \langle t \rangle] @ c \Leftrightarrow \langle s' \rangle[b \mapsto \langle t \rangle] @ c \rangle) && \text{Lemma 4.11 } c \# \langle s \rangle, \langle s' \rangle, \langle t \rangle \\ &= \text{all}[c](\langle \langle s[b:=t] \rangle @ c \Leftrightarrow \langle s'[b:=t] \rangle @ c \rangle) && \text{IH } \text{size}(s), \text{size}(t) < \text{size}(s=t) \\ &= \langle s[b:=t] = s'[b:=t] \rangle && \text{Figure 8} \\ &= \langle (s=s')[b:=t] \rangle && \text{Fact of syntax}\end{aligned}$$

— *The case of b .* By Figure 8 $\langle b \rangle = \text{atm}(b)$. By assumption $\langle t \rangle \in \text{Set}^{\text{level}(b)}$ so by Figure 1 ($\sigma\alpha$)

$$\text{atm}(b)[b \mapsto \langle t \rangle] = \langle t \rangle.$$

— *The case of a (any atom other than b).* By Figure 8 $\langle a \rangle = \text{atm}(a)$. We use rule ($\sigma\mathbf{b}$) of Figure 1.

— *The case of $\{a \mid \phi\}$.* α -converting if necessary assume a is fresh (so $a \# t$, and by Theorem 2.31 also $a \# \langle t \rangle$). We reason as follows:

$$\begin{aligned}\langle \{a \mid \phi\} \rangle[b \mapsto \langle t \rangle] &= ([a](\langle \phi \rangle)[b \mapsto \langle t \rangle]) && \text{Figure 8} \\ &= [a](\langle \phi \rangle[b \mapsto \langle t \rangle]) && \text{Figure 1 } (\sigma[]), a \# \langle t \rangle \\ &= [a](\langle \phi[b:=t] \rangle) && \text{IH } \text{size}(\phi) < \text{size}(\{a \mid \phi\}) \\ &= \langle \{a \mid \phi[b:=t]\} \rangle && \text{Figure 8, } a \# t \\ &= \langle \{a \mid \phi\}[b:=t] \rangle && \text{Fact of syntax}\end{aligned}$$

— *The case of $t' \in s'$.* Choose fresh $b' \in \mathbb{A}^{\text{level}(t')}$ (so $b' \# t', s', t$, and by Theorem 2.31 $b' \# \langle t \rangle, s'[b:=t], t'[b:=t]$).

$$\begin{aligned}\langle t' \in s' \rangle[b \mapsto \langle t \rangle] &= (\langle s' \rangle @ b')[b' \mapsto \langle t' \rangle][b \mapsto \langle t \rangle] && \text{Fig 8, Ntn 6.1, } b' \# s' \\ &= (\langle s' \rangle @ b')[b \mapsto \langle t \rangle][b' \mapsto \langle t' \rangle][b \mapsto \langle t \rangle] && \text{Lemma 4.12, } b' \# \langle t \rangle \\ &= (\langle s' \rangle @ b')[b \mapsto \langle t \rangle][b' \mapsto \langle t' [b:=t] \rangle] && \text{IH } \text{size}(t') < \text{size}(t' \in s') \\ &= (\langle s' \rangle[b \mapsto \langle t \rangle] @ b')[b' \mapsto \langle t' [b:=t] \rangle] && \text{Lemma 4.11, } b' \# \langle t \rangle \\ &= (\langle s'[b:=t] \rangle @ b')[b' \mapsto \langle t' [b:=t] \rangle] && \text{IH } \text{size}(s') < \text{size}(t' \in s') \\ &= \langle t' [b:=t] \in s' [b:=t] \rangle && \text{Fig 8, Ntn 6.1, } b' \# s' [b:=t], t' [b:=t] \quad \square\end{aligned}$$

LEMMA 9.13. Suppose ϕ is a stratified formula and s is a stratified term. Suppose $a \in \mathbb{A}^{i+1}$ and $\text{level}(s) = i$. Then

$$\langle s \in \{a \mid \phi\} \rangle = \langle \phi[a := s] \rangle.$$

Proof. We reason as follows:

$$\begin{aligned} \langle s \in \{a \mid \phi\} \rangle &= (([a] \langle \phi \rangle) @ a) [a \mapsto \langle s \rangle] && \text{Fig 8 \& Ntn 6.1} \\ &= \langle \phi \rangle [a \mapsto \langle s \rangle] && \text{Lemma 2.66(1)} \\ &= \langle \phi[a := s] \rangle && \text{Lemma 9.12} \end{aligned} \quad \square$$

9.4. The denotation of a formula

Recall $\langle - \rangle$ from Definition 9.7 and $[-]$ from Notation 8.6:

DEFINITION 9.14. Suppose ϕ is a stratified formula and s is a stratified term (Subsection 9.1). Define $[\phi]$ and $[s]$ by

$$[\phi] = \llbracket \langle \phi \rangle \rrbracket \quad \text{and} \quad [s] = \llbracket \langle s \rangle \rrbracket.$$

LEMMA 9.15. Suppose ϕ and ψ are stratified formulae and $p \in \text{Pnt}$. Then:

- (1) $[\perp] = \emptyset$.
- (2) $[\phi \Rightarrow \psi] = (\text{Pnt} \setminus [\phi]) \cup [\psi]$.

Proof. For part 1 we note by Definition 9.14, Figure 8, and Lemma 5.9(3) that

$$[\perp] = \llbracket \langle \perp \rangle \rrbracket = \llbracket \text{false} \rrbracket = \emptyset.$$

Part 2 is similar, from Notation 6.1. \square

LEMMA 9.16. Suppose ϕ and ψ are stratified formulae and s is a stratified term. Suppose $a \in \mathbb{A}^i$ and $\text{level}(s) = i$. Then:

- (1) If $[\phi] = \text{Pnt}$ then $[\forall a. \phi] = \text{Pnt}$.
- (2) $[\forall a. \phi] \subseteq [\phi[a := s]]$.
- (3) If $a \# \phi$ then $[\forall a. (\phi \Rightarrow \psi)] \subseteq [\phi \Rightarrow \forall a. \psi]$.

Proof. Note by Lemma 8.5 that $a \# \text{Pnt}$. Part 1 follows from Lemma 8.11.

For part 2, note by Lemma 9.10 that $[s] \in \text{Set}^i$ and the σ -action $[a \mapsto [s]]$ from Definition 4.1 is well-defined. We reason as follows:

$$\begin{aligned} [\forall a. \phi] &= [\text{all}[a] \langle \phi \rangle] && \text{Figure 8} \\ &\subseteq [\langle \phi \rangle [a \mapsto [s]]] && \text{Lemma 8.14} \\ &= [\phi[a := s]] && \text{Lemma 9.12} \end{aligned}$$

For part 3 we unpack Notation 6.1, we note by Theorem 2.31 that $a \# \langle \phi \rangle$, and we reason using Figure 8 and Lemma 8.12. \square

LEMMA 9.17. Suppose s is a stratified term. Then $[s = s] = \text{Pnt}$.

Proof. Choose fresh $c \in \text{level}(s) - 1$ (so $c \# s$). We unpack Definition 9.14 and Figure 8 and see that we need to check that $\text{Pnt} = [\forall c. \text{iff}(\langle s \rangle @ c, \langle s \rangle @ c)]$ where iff is from Notation 6.1. By Lemma 8.11(2) it would suffice to check that $\text{Pnt} = [\text{iff}(\langle s \rangle @ c, \langle s \rangle @ c)]$. Now we unpack Notation 6.1 and Figure 3 and see that this holds if $[\langle s \rangle] @ c \subseteq [\langle s \rangle] @ c$, and this is indeed true. \square

9.5. Consistency of TST, if points exist

Theorem 9.18 makes formal that the denotation $[-]$ from Definition 9.14 is sound for TST:

THEOREM 9.18. Suppose ϕ is a stratified formula. Then if $\vdash \phi$ is derivable in TST then $[\phi] = \text{Pnt}$.

Proof. We consider each of the rules and axioms of Figure 6:

- (**modus ponens**) is a fact of sets: if $\llbracket \phi \rrbracket = \text{Pnt}$ and $\llbracket \phi \Rightarrow \psi \rrbracket = \text{Pnt}$ then $(\llbracket \phi \rrbracket \subseteq \llbracket \psi \rrbracket)$ and therefore $\llbracket \psi \rrbracket = \text{Pnt}$.
- (**generalisation**) and (**instantiation**) and (**allR**) are from Lemma 9.16.
- (**K**), (**S**), and (**contrapositive**) are by Lemma 9.15 and properties of sets membership.
- (**identity**) is Lemma 9.17.
- (**Leibniz**) is Theorem 8.20 (and Lemma 9.12).
- (**extensionality**) is by construction from Figures 6 and 8.
- (**comprehension**) is Lemma 9.13. □

COROLLARY 9.19. *If $\text{Pnt} \neq \emptyset$ then $\vdash \perp$ is not derivable in TST. In words: TST is consistent, provided that points exist.*

Proof. We prove the contrapositive. Suppose $\vdash \perp$ is derivable. By Theorem 9.18 this would imply that Pnt is equal to $\llbracket \perp \rrbracket$ which by Lemma 9.15(1) means $\text{Pnt} = \emptyset$. □

REMARK 9.20. We know TST is consistent anyway: it suffices to choose a set U to denote level 1, and to denote level $i+1$ with the powerset of the denotation of level i . Given a valuation for the variables, sets are denoted by sets and predicates by truth-values. Call this the **sets and powersets** semantics of TST.

Still, the model we have given is arguably elegant, and it has some special features:

- It dispenses with valuations, giving denotations directly to terms and predicates whether open or closed¹⁶, and denotes sets by the atoms-abstraction of the denotation of predicates.
- In the next Section we show this is also a model of TST+, and we did not know that before.

EXAMPLE 9.21. It is interesting to continue Remark 9.20 and compare and contrast the sets and powersets TST model for $\{a \mid \top\}$ with that provided by the nominal representation of this paper.

- The sets and powersets model of $\{a \mid \top\}$ is the set $pset^{level(a)}(U)$.
- Figure 3 gives $[a]\text{Pnt}$ (the atoms-abstraction by a of the set of all points).
- Given any (pre)point p , Definition 6.2 gives $\text{Set}^{level(a)}$ (the set of all internal sets with the same level as a).

By Lemma 8.5 $a \# \text{Pnt}$ so that the atoms-abstraction is vacuous. Formally: by Lemma 2.64 and Corollary 2.28 $[a]\text{Pnt} = [a']\text{Pnt}$ for every other $a' \in \mathbb{A}^{level(a)}$. So $[a]\text{Pnt}$ forgets the name and remembers only the level of a and can be viewed as expressing ‘ Pnt , served up as a level i set’.

Also, Set^i is isomorphic to Set^j for any i and j , by shifting levels of atoms by $i-j$. So Set^i can be viewed as expressing ‘all internal sets, viewed from level i ’.

Thus, $[a]\text{Pnt}$ and $\text{Set}^{level(a)}$ change little or not at all when the name or the level of the bound atom changes, whereas the set $pset^{level(a)}(U)$ changes significantly by becoming larger and smaller. Both are reasonable models of ‘a universal set’, but the denotations used in this paper come visibly closer to being a model of ‘the universal set’—and arguably they come as close as it is possible to come, in a stratified language.

9.6. Consistency of TST+, if points exist

DEFINITION 9.22. Call a formula ϕ (Subsection 9.1) **closed** when $\text{supp}(\phi) = \emptyset$.

REMARK 9.23. ϕ is closed in the sense of Definition 9.22 exactly when it is closed when viewed as a logical predicate, that is, when it has no free atoms / no free variables.

DEFINITION 9.24. If ϕ is a closed formula write ϕ^+ for the formula that is syntactically identical to ϕ except that all the levels of all bound atoms have been incremented by one.

¹⁶Following the terminology of [DG12a; Gab16] we call this denotation *absolute*.

An inductive definition of ϕ^+ is possible, however, giving two examples seems shorter and clearer: if $a, a' \in \mathbb{A}^i$ and $b, b' \in \mathbb{A}^{i+1}$ then

$$(\forall a. a=a)^+ = \forall b. b=b \quad \text{and} \quad (\forall a'. \{a | a=a'\} = \{a | a'=a\})^+ = \forall b'. \{b | b=b'\} = \{b | b'=b\}.$$

DEFINITION 9.25. The language of TST+ is identical to the language to TST (Definition 9.4) and has all the TST axioms and derivation rules from Figure 6.

In addition TST+ has the **typical ambiguity** axiom scheme: for each stratified closed formulae ϕ we assume an axiom (TA) from Figure 7; for the reader's convenience we duplicate it here:

$$(TA) \quad \vdash \phi \Rightarrow \phi^+.$$

REMARK 9.26. Typical ambiguity allows us to consistently 'raise' and 'lower' the level of atoms. All the atoms must be raised together by the same amount.

Note that we can do this from within a derivation (not just as a property of derivations), because we have an axiom asserting the implication. A concise but clear presentation of typical ambiguity is in [Wan81, page 92], see also [Spe62, page 119].

REMARK 9.27. NF is known consistent relative to TST+ (the proof is summarised in [Spe62], a more detailed account in German is in the final three pages of [Spe58]). So, to prove consistency of NF it suffices to consider TST+.

The relative consistency is intuitively reasonable: NF and TST differ in that TST's language is *stratified* whereas NF's is *stratifiable*—stratifications exist, but we do not say which one. So it is reasonable that NF should be equivalent to TST plus axioms that allow us to adjust our stratification on-the-fly to another possible stratification, if we so choose.

THEOREM 9.28. *Suppose ϕ is a stratified closed formulae (Definitions 9.2 & 9.22). Then*

$$[\phi] = [\phi^+].$$

Proof. Consider some point $p \in [\phi]$. By clause 3 of Definition 8.3 p is ambiguous, so there exists a shift permutation (Definition 2.13) ϑ such that $\vartheta \cdot p = p$. Since ϕ is closed and ϑ maps \mathbb{A}^i to \mathbb{A}^{i+1} for every $i \in \mathbb{Z}$, we see that $\vartheta \cdot \phi = \phi^+$.

We now reason as follows:

$$\begin{aligned} p \in [\phi] &\Leftrightarrow \vartheta \cdot p \in [\phi] && p \text{ ambiguous} \\ &\Leftrightarrow p \in \vartheta \cdot [\phi] && \text{Theorem 2.31} \\ &\Leftrightarrow p \in [\vartheta \cdot \phi] && \text{Theorem 2.31} \\ &\Leftrightarrow p \in [\phi^+] && \vartheta \cdot \phi = \phi^+ \end{aligned}$$

Thus $[\phi] \subseteq [\phi^+]$. The reverse subset inclusion follows similarly. □

REMARK 9.29. We never use the fact that $0 \in \mathbb{Z}$ is actually the number zero; our interest in \mathbb{Z} is just this: that it is totally ordered, with a translational symmetry given by taking successor, and for any $i \in \mathbb{Z}$ the subset $\{i' \in \mathbb{Z} \mid i' \geq i\}$ is well-founded (so we can define *minlevel* in Definition 4.4).

COROLLARY 9.30. *If $\text{Pnt} \neq \emptyset$ (in words: if a point exists) then $\vdash \perp$ is not derivable in TST+. In words: TST+ is consistent, provided that points exist.*

Proof. Just as the proof of Corollary 9.19, using Theorems 9.18 and 9.28. □

So we just need to construct some point—any point—and this will suffice to deduce consistency of NF. We do this next, culminating with Theorem 12.52.

10. THEORIES

10.1. The basic definition

DEFINITION 10.1. Call $T \subseteq \bigcup_{i \in \mathbb{Z}} \text{Set}^i \times \text{Set}^i$ a(n equality) theory.

Call T **small** when $\#T < T_\omega$ (Definition 2.1).

It would be more descriptive to call a theory T a **stratified relation**—because that is what it is. However, what we *do* with T makes most sense if we think of it as an equality theory.

We extend Definition 7.1:

DEFINITION 10.2. Suppose T is a theory and $j \in \mathbb{Z}$ and $\mathcal{Y} \subseteq \text{Set}^j$. Then define $\mathcal{Y} \models_\lambda T$ by

$$\mathcal{Y} \models_\lambda T \text{ when } \forall (u, u') \in T. \mathcal{Y} \models u = u'.$$

Recall $p \models u = u'$ and $p \Vdash u = u'$ from Definition 7.2:

DEFINITION 10.3. Suppose T is a theory and suppose $p \in \text{PrPt}$. Define $p \models_\lambda T$ and $p \Vdash_\lambda T$ and $p \models_{\nabla} T$ and $p \Vdash_{\nabla} T$ by

$$\begin{aligned} p \models_\lambda T & \text{ when } \forall (u, u') \in T. p \models u = u' \\ p \Vdash_\lambda T & \text{ when } \forall (u, u') \in T. p \Vdash u = u' \\ p \models_{\nabla} T & \text{ when } \exists (u, u') \in T. p \models u = u' \\ p \Vdash_{\nabla} T & \text{ when } \neg(p \models_{\nabla} T). \end{aligned}$$

REMARK 10.4. We have accumulated several levels of definitions by this point, so it might help to unpack them. Unpacking Definitions 10.3 and 7.2 and 7.1 we see that:

— $p \models_\lambda T$ when for every $(u, u') \in T$ and $a \in \mathbb{A}$, $pa \models u = u'$.

— $p \models_\lambda T$ when for every $(u, u') \in T$ and $z \in \text{Set}$ and $c \in \mathbb{A}^{\text{level}(u)}$ and $a \in \mathbb{A}^{\text{level}(z)+1}$, we have

$$p \models z[c \mapsto u] \in a \quad \text{if and only if} \quad p \models z[c \mapsto u'] \in a.$$

— We can unpack \in from Notation 6.1 and (**modelt**) from Figure 3 and note that $p \models z[c \mapsto u] \in a$ when $a \circ z[c \mapsto u] \in p$, and similarly for $z[c \mapsto u'] \in a$.

— $p \Vdash_\lambda T$ when for every $(u, u') \in T$ there exists an $a \in \mathbb{A}$ such that $pa \not\models u = u'$.

— $p \Vdash_{\nabla} T$ when for every $(u, u') \in T$ there exist $z \in \text{Set}$ and $c \in \mathbb{A}^{\text{level}(u)}$ and $a \in \mathbb{A}^{\text{level}(z)+1}$, such that

$$p \models z[c \mapsto u] \in a \quad \text{and} \quad p \not\models z[c \mapsto u'] \in a,$$

or vice versa.

Lemmas 10.5 and 10.6 are not hard and will be useful later:

LEMMA 10.5. Suppose T is a theory and $p \in \text{PrPt}$. Then

$$p \models_\lambda T \Leftrightarrow \forall a \in \mathbb{A}. pa \models_\lambda T.$$

Proof. From Definitions 7.2 and 10.3. □

LEMMA 10.6. Suppose T is a theory and $p \in \text{PrPt}$. Suppose $i \in \mathbb{Z}$ and $x \in \text{Set}^i$. Then

$$p \models_\lambda T \wedge p \Vdash_\lambda T \text{ implies } px \models_\lambda T.$$

Proof. Consider $(u, u') \in T$ and suppose $a \in \mathbb{A}^{\text{level}(u)}$ and $y \in \text{Set}^{i-1}$. By Proposition 7.5 and Definition 6.2 $y[a \mapsto u] \in px \Leftrightarrow y[a \mapsto u'] \in px$. □

REMARK 10.7. Given a theory P we obtain a prepoint p by considering

$$\{a \circ u \mid i \in \mathbb{Z}, a \in \mathbb{A}^{i+1}, u \in \text{Set}^i, b \in \mathbb{A}^0, b \# u, (\{b \mid u \in a\}, \{b \mid T\}) \in P\}.$$

Above, b is a fresh ‘dummy atom’ which is required to convert internal predicates $u \in a$ and T into internal sets.

So p ‘believes’ $u \in a$ when P asserts, intuitively, that $u \in a$ is equal to true.

Conversely given a prepoint p we obtain an equality theory P by considering

$$\{(u, v) \mid i \in \mathbb{Z}, u, v \in \text{Set}^i, p \Vdash u=v\}.$$

So P ‘believes’ that $u=v$ when, at p , they are extensionally equal.

This suggests that equality theories are prepoints in disguise, and vice versa, or at least, that some quite strong equivalence should hold between them.¹⁷

The interested reader can find part of this intuition made formal later in Subsection 10.4 by Definition 10.18 and Lemma 10.20(2).

Remaining at a high level for now, we can ask: equality theories and prepoints are clearly closely related, and we shall certainly see that we move between them in what follows, so why do we need both?

The answer is that the construction of an extensional equality theory in Definition 11.19 seems more convenient if we use equality theories, but it is easier to work with (pre)points elsewhere, such as in Figure 3 and all that depends on it.

So intuitively, an extensional equality = ‘wants’ us to use equality theories, but the rest of the logical structure (σ and \forall , for instance) ‘wants’ us to use points. We use equality theories *and* (pre)points because our logic contains an extensional equality *and* a universal quantifier.

10.2. Deductive closure

Recall from Definition 10.1 the notion of a *theory*:

DEFINITION 10.8. Call a theory C a **congruence** when

- (1) C is an equivalence relation (transitive, reflexive, symmetric), and
- (2) if $i, k \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $a \in \mathbb{A}^i$ and $z \in \text{Set}^k$ then

$$(u, u') \in C \quad \text{implies} \quad (z[a \mapsto u], z[a \mapsto u']) \in C.$$

Whenever we write ‘congruence’ below, we mean a theory that is a congruence in the sense of Definition 10.8.

REMARK 10.9. The reader can compare clause 2 with Proposition 7.5(2); we exploit the similarity in Lemma 10.21. Note also that Definition 10.8 does not include a rule

$$(z, z') \in C \quad \text{implies} \quad (z[a \mapsto u], z'[a \mapsto u]) \in C.$$

DEFINITION 10.10. Suppose T is a theory.

- (1) Define $[T]_{\text{eq}}$ the **deductive closure** of T to be the least congruence containing T .
- (2) If $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$ then write

$$T \models^{\text{eq}} x=x' \quad \text{when} \quad (x, x') \in [T]_{\text{eq}}.$$

- (3) If $i \in \mathbb{Z}$ and $x \in \text{Set}^i$ then define

$$\begin{aligned} [x]_T &= \{x' \in \text{Set}^i \mid T \models^{\text{eq}} x=x'\} \quad \text{or equivalently} \\ [x]_T &= \{x' \in \text{Set}^i \mid (x, x') \in [T]_{\text{eq}}\}. \end{aligned}$$

- (4) If $i \in \mathbb{Z}$ and $\mathcal{X} \subseteq \text{Set}^i$ then define

$$\begin{aligned} [\mathcal{X}]_T &= \bigcup \{[x]_T \mid x \in \mathcal{X}\} \quad \text{or equivalently} \\ [\mathcal{X}]_T &= \{x' \in \text{Set}^i \mid x \in \mathcal{X}, T \models^{\text{eq}} x = x'\} \end{aligned}$$

LEMMA 10.11(1) Suppose T is a theory. Then $T \subseteq [T]_{\text{eq}}$.

- (2) Suppose T and T' are theories. Then $T \subseteq T'$ implies $[T]_{\text{eq}} \subseteq [T']_{\text{eq}}$.

¹⁷Some well-behavedness conditions are certainly necessary. For instance, the theory P should be such that the *level* of b does not matter for the result we obtain. But this is entirely reasonable.

(3) Suppose $(T_\gamma)_\gamma$ is an ascending chain of theories ordered by subset inclusion. Then $[\bigcup_\gamma T_\gamma]_{\text{eq}} = \bigcup_\gamma [T_\gamma]_{\text{eq}}$.

Proof. By routine calculations from Definition 10.10. □

Recall \models from Definition 7.1 and $\models_{\mathcal{A}}$ from Definition 10.2:

LEMMA 10.12. Suppose T is a theory and $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$ and $\mathcal{X} \subseteq \text{Set}^i$. Then:

- (1) $[x]_T \models_{\mathcal{A}} T$ and $[\mathcal{X}]_T \models_{\mathcal{A}} T$.
- (2) $[[\mathcal{X}]_T]_T = [\mathcal{X}]_T$.
- (3) $\emptyset \models_{\mathcal{A}} T$.

Proof. (1) We unpack Definitions 10.2 and 7.1 and consider any $z \in [x]_T$ and $(u, u') \in [T]_{\text{eq}}$, and we reason as follows:

$$\begin{aligned} z[a \mapsto u] \in [x]_T &\Leftrightarrow (x, z[a \mapsto u]) \in [T]_{\text{eq}} && \text{Definition 10.10} \\ &\Leftrightarrow (x, z[a \mapsto u']) \in [T]_{\text{eq}} && \text{Definition 10.8(1\&2)} \\ &\Leftrightarrow z[a \mapsto u'] \in [x]_T && \text{Definition 10.10} \end{aligned}$$

The reasoning for \mathcal{X} is no harder.

- (2) By a routine calculation using transitivity in Definition 10.8(1).
- (3) This follows noting of Definition 10.10(4) that $[\emptyset]_T = \emptyset$. □

10.3. Further properties of small theories

This subsection will help us in Proposition 11.30, in which we will consider an ascending chain of small (Definition 10.1) theories.

Small theories have special properties, as described in Lemma 10.15 and Corollary 10.16.

First, we note Notation 10.13 and Lemma 10.14 which will be helpful in Lemma 10.14, and also later in Proposition 11.30:

NOTATION 10.13. Suppose T is a theory (Definition 10.1) and $i \in \mathbb{Z}$ and $u \in \text{Set}^i$ is an internal set. Say

$$u \text{ appears in } T \text{ when } \exists u' \in \text{Set}^i. (u = u' \in T \vee u' = u \in T).$$

LEMMA 10.14. Suppose T is a small theory and $a \in \mathbb{A}$. Then:

- (1) $\text{supp}(T) = \bigcup \{ \text{supp}(u) \mid u \text{ appears in } T \}$.
- (2) $a \# T$ if and only if $a \# u$ for every $u \in \text{Set}$ that appears in T .

Proof. Direct from Lemma 2.51(2) and Subsection 2.2.2. □

LEMMA 10.15. Suppose T is a small theory and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Suppose $a \# T$ and $a \# x$. Then

$$(a, x) \notin [T]_{\text{eq}}.$$

Proof. By a routine induction on $[T]_{\text{eq}}$. The base case is that $(a, x) \in [T]_{\text{eq}}$ because of clause 2 of Definition 10.8, so that $a = z[a' \mapsto u]$ and $x = z[a' \mapsto u']$ for some $(u, u') \in T$. We examine (modatm) and (modset) in Figure 3 and see that there are two sub-cases:

- Suppose $z = a$. Then also $x = a$, contradicting our assumption that $a \# x$.
- Suppose $z = a'$. Then $u = a$, contradicting our assumption that $a \# T$ by Lemma 10.14(2). □

COROLLARY 10.16. Suppose T is a small theory and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and $a \# T$. Then:

- (1) If $x \in [a]_T$ then $a \in \text{supp}(x)$.
- (2) If $a \# x$ then $x \notin [a]_T$.

Proof. For part 1, from Definition 10.10(2) $x \in [a]_{\top}$ precisely when $(a, x) \in [\top]_{\text{eq}}$. By Lemma 10.15 (since \top is small and $a \# \top$) $\neg(a \# \top)$ —that is, $a \in \text{supp}(x)$.

Part 2 is just the contrapositive. \square

10.4. The syntactic prepoint

Given a logical theory it is standard to build a model out of syntax quotiented by derivable equivalence. In this subsection, we consider an appropriate construction for equality theories. Interestingly, we make good use of the shift permutation ϑ .

Notation 10.17 does for *sets* of internal sets what the similar terminology from Definition 8.3 did for internal sets:

NOTATION 10.17. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $\mathcal{X} \subseteq \text{Set}^i$.

- Say p **names** \mathcal{X} using $a \in \mathbb{A}^{i+1}$ when $pa = \mathcal{X}$.
- Say p **names** \mathcal{X} when there exists some $a \in \mathbb{A}^{i+1}$ such that $pa = \mathcal{X}$.

DEFINITION 10.18. Suppose ϑ is a shift permutation (Definition 2.13) and suppose P is a ϑ -ambiguous theory (so $\vartheta \cdot P = P$). Then define the **Herbrand prepoint** $\text{herb}(P) \in \text{PrPt}$ by

$$\text{herb}(P)(\vartheta(a)) = [a]_P.$$

Or equivalently:

$$\begin{aligned} \text{herb}(P) &= \{ \vartheta(a) \circ x \mid i \in \mathbb{Z}, a \in \mathbb{A}^i, x \in \text{Set}^i, (a, x) \in [P]_{\text{eq}} \} \\ x \in \text{herb}(P)(a') &\Leftrightarrow (x, \vartheta^{-1}(a')) \in [P]_{\text{eq}} \quad (a' \in \mathbb{A}, x \in \text{Set}^{\text{level}(a')-1}) \end{aligned}$$

REMARK 10.19. In light of Notation 10.17 we can say that $\text{herb}(P)$ names $[a]_P$ using $\vartheta(a)$.

We call $\text{herb}(P)$ after Herbrand models, because it associates to $\vartheta(a)$ the equivalence class of a under derivable equality. We hope this terminology and analogy will be helpful, but it is imperfect and there is some danger of inadvertently misleading the reader:

- (1) We do not restrict to ground terms; Herbrand models do.
- (2) There is important extra structure: the shift permutation ϑ is involved, neatly, in assigning $\vartheta(a)$ as a name to $[a]_P$.
We cannot assign a to name $[a]_P$ because we need an atom in $\text{level}(a)+1$. So ϑ was introduced to ensure ambiguity, but here it also makes itself positively useful and helps us to build those models.
- (3) It may be worth noting that in this paper, internal sets (which correspond to ‘terms’) and internal predicates (which correspond to ‘predicates’) are—up to gaining or losing an abstracted atom—the same structure.

So even though $\text{herb}(P)$ is not a Herbrand construction, the spirit of the idea is related, and for want of a better name we abuse terminology and call it ‘Herbrand prepoint’.¹⁸

LEMMA 10.20. Suppose ϑ is a shift permutation (Definition 2.13) and suppose P is ϑ -ambiguous theory (so $\vartheta \cdot P = P$). We have the following:

- (1) $\vartheta \cdot \text{herb}(P) = \text{herb}(P)$.
- (2) $\text{herb}(P) \models_{\lambda} P$.

Proof. (1) From Theorem 2.31 and our assumption in Definition 10.18 that $\vartheta \cdot P = P$.

- (2) By construction using Lemma 10.12(1) (see Remark 10.4). \square

The interested reader can compare Lemma 10.20 to a later sequel to the result which is Lemma 11.32.

¹⁸We also mention Lindenbaum-Tarski algebras, which resemble Herbrand models. They do not insist on closed syntax but consist of predicates quotiented by derivable equivalence rather than terms quotiented by derivable equality.

10.5. A sanity check

We take a moment to prove two sanity checks on deductive closure:

LEMMA 10.21. *Suppose $p \in \text{PrPt}$. Then:*

(1) *Suppose $i, k \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $z \in \text{Set}^k$. Then*

$$p \models u=u' \wedge p \Vdash u=u' \text{ implies } p(z[a \mapsto u]) = p(z[a \mapsto u']).$$

(2) *Suppose \top is a theory. Then*

$$p \models_{\bar{\lambda}} \top \wedge p \Vdash_{\bar{\lambda}} \top \text{ implies } p \models_{\bar{\lambda}} [\top]_{\text{eq}}.$$

Proof. For part 1, we suppose $p \models u=u'$ and $p \Vdash u=u'$ and consider $y \in \text{Set}^{k-1}$ and we reason as follows:

$$\begin{aligned} y \in p(z[a \mapsto u]) &\Leftrightarrow p \models y \in (z[a \mapsto u]) && \text{Definition 6.2} \\ &\Leftrightarrow p \models y \in (z[a \mapsto u']) && \text{Prop 7.5(2), } p \models u=u', p \Vdash u=u' \\ &\Leftrightarrow y \in p(z[a \mapsto u']) && \text{Definition 6.2} \end{aligned}$$

Part 2 follows by induction on Definition 10.8, using the fact that sets equality is an equivalence relation for Definition 10.8(1), and using part 1 of this result for Definition 10.8(2). \square

The reader who likes proofs by contradiction and examples based on the empty set is now in for a treat:

COROLLARY 10.22. *Suppose $i \in \mathbb{Z}$ and write \emptyset for the empty equality theory. Then*

$$\emptyset \not\models^{\text{eq}} \text{empt}^i = \text{set}^i.$$

Proof. Consider the empty equality theory \emptyset and the empty point $\emptyset \in \text{PrPt}$. Clearly $\emptyset \models_{\bar{\lambda}} \emptyset$ and $\emptyset \Vdash_{\bar{\lambda}} \emptyset$, therefore by Lemma 10.21 $\emptyset \models_{\bar{\lambda}} [\emptyset]_{\text{eq}}$. Then if $\emptyset \models^{\text{eq}} \text{empt}^i = \text{set}^i$ then $(\text{empt}^i, \text{set}^i) \in [\emptyset]_{\text{eq}}$ and therefore $\emptyset \Vdash \text{empt}^i = \text{set}^i$. But this contradicts Lemma 6.12. \square

10.6. Counting subsets

REMARK 10.23. In Proposition 11.30 it will be important to be able to biject atoms with internal sets, and also to biject atoms with sets of internal sets—we may say the atom *names* them (Notation 10.17).

It is important not to run out of atoms while constructing these bijections. Proposition 11.5 makes this precise and formal. The proof uses Lemmas 10.26 and 10.27.

NOTATION 10.24. Suppose $i \in \mathbb{Z}$ and $x \in \text{Set}^i$. Suppose $A \subseteq \mathbb{A}$. Then write:

- (1) $\text{fix}(A) \cdot x = \{\pi \cdot x \mid \pi \in \text{fix}(A)\}$ and call this the $\text{fix}(A)$ -**orbit** of x .
- (2) $\text{Orb}(x) = \text{fix}(\emptyset) \cdot x = \{\pi \cdot x \mid \pi \text{ any permutation}\}$ and call this the **(full) permutation orbit** of x .

Lemma 10.25 generalises Lemma 2.45:

LEMMA 10.25. *Suppose $i \in \mathbb{Z}$ and $\mathcal{X} \subseteq \text{Set}^i$ is small supported and $x \in \text{Set}^i$. Suppose $A \subseteq \mathbb{A}$ and $\text{supp}(\mathcal{X}) \subseteq A$. Then*

$$x \in \mathcal{X} \Leftrightarrow \text{fix}(A) \cdot x \subseteq \mathcal{X}.$$

So x is in \mathcal{X} if and only if its orbit is in \mathcal{X} .

Proof. By Theorem 2.31 and Corollary 2.28(1), $x \in \mathcal{X}$ if and only if $\pi \cdot x \in \mathcal{X}$, for any $\pi \in \text{fix}(A)$. \square

LEMMA 10.26. *Suppose $i \in \mathbb{Z}$. Then there are \top_1 many equivariant (Definition 2.44) subsets of Set^i .*

Proof. Consider some equivariant $\mathcal{X} \subseteq \text{Set}^i$ and recall from Definition 2.44 that \mathcal{X} is equivariant when $\text{supp}(\mathcal{X}) \subseteq \emptyset$. For the purposes of counting \mathcal{X} , it suffices to count the possibilities for whether $x \in \mathcal{X}$ or $x \notin \mathcal{X}$ for all possible $x \in \text{Set}$.

By Lemma 10.25 taking $A = \emptyset$ it suffices to count the possibilities for whether full permutation orbits $\text{fix}(\emptyset) \cdot x = \text{Orb}(x)$ are in \mathcal{X} .

We see that the size of \mathbb{A} is irrelevant because orbits are equivalence classes under all permutative renamings of atoms. The orbits behave like generalised α -equivalence classes and for each orbit, free atoms in representatives x behave as if they are α -bound, in no particular order, at top level.¹⁹

The syntactic structure of x (the constructors `elt`, `and`, `all`, and `[a]`- from Definition 3.1) is countable and can be enumerated. So for the purposes of counting subsets, it suffices to count the subsets of ω . The result follows. \square

LEMMA 10.27. *Suppose $\mathcal{A} \subseteq \mathbb{A}$ is a set of atoms such that $\top_1 \leq \#\mathcal{A} < \top_\omega$ —so \mathcal{A} is uncountable, but is still small (Notation 2.6).*

Suppose $i \in \mathbb{Z}$. Then there are $2^{\#\mathcal{A}}$ many subsets of Set^i with support in \mathcal{A} . In symbols:

$$\#\{X \subseteq \text{Set}^i \mid \text{supp}(X) \subseteq \mathcal{A}\} = 2^{\#\mathcal{A}}.$$

Proof. Consider $\mathcal{X} \subseteq \text{Set}^i$ with $\text{supp}(\mathcal{X}) \subseteq \mathcal{A}$ and consider any $x \in \text{Set}^i$.

For the purposes of counting \mathcal{X} , it suffices to count the possibilities for whether $x \in \mathcal{X}$ or $x \notin \mathcal{X}$. We note two things:

- (1) Using Lemma 10.25 (much as we did in the proof of Lemma 10.26) it suffices to count possible $\text{fix}(\mathcal{A})$ -orbits, which are equivalence classes up to renaming atoms not in \mathcal{A} . Thus we may treat free atoms in x in $\text{supp}(x) \setminus \mathcal{A}$ as if they are α -bound, in no particular order, at top level.
- (2) Also for our purposes here, the terms structure of x (the constructors `elt`, `and`, `all`, and `[a]`- from Definition 3.1) is countable and is swamped by the size of \mathcal{A} which we assumed is uncountable. Thus we may disregard the terms structure.

So to count how many $\mathcal{X} \subseteq \text{Set}^i$ exist with $\text{supp}(\mathcal{X}) \subseteq \mathcal{A}$ it suffices to count the possibilities for $\text{supp}(\mathcal{X}) \subseteq \mathcal{A}$, that is, it suffices to count the number of subsets of \mathcal{A} . Thus we obtain $2^{\#\mathcal{A}}$. \square

REMARK 10.28. Lemma 10.27 is related to a known and useful property of nominal powersets. In nominal techniques as presented in [GP01], nominal sets have finite support and the set of atoms is countably infinite. Then $\text{pset}_{\text{finsupp}}(\mathbb{A})$, the set of finitely-supported sets of atoms, consists of finite and cofinite sets of atoms. Since we assume countably infinitely many atoms, $\#\mathbb{A} = \#\text{pset}_{\text{finsupp}}(\mathbb{A})$.

Lemma 10.27 is about Set^i which is a more complex datatype than atoms, and it assumes a larger set of atoms and a larger notion of ‘small support’. Nevertheless, if it helps, the reader can view Lemma 10.27 as being just the observation from the previous paragraph, scaled up.

Lemmas 10.26 and 10.27 are used to prove Proposition 11.5 below. We need just a little more machinery to state it.

11. EXTENSIONALITY

In Definition 11.19 we construct a particular equality theory ext with three very nice properties given in Lemma 11.20, Corollary 11.26, and Proposition 11.30:

- Corollary 11.26 expresses that any prepoint validating ext must also satisfy clause 2 of Definition 8.3, which is one of the conditions for being a point.
- Proposition 11.30 is clearly related to clause 1 of Definition 8.3. Prepoints exist that validate ext and do *not* satisfy clause 1, however, we will deal with that in later sections and we will do so using Proposition 11.30.

¹⁹ A nominal binder for this with a theory of rewriting was considered in [FG05].

- Lemma 11.20 states that ext is ϑ -ambiguous, which is clearly related to clause 3 of Definition 8.3. Again, prepoints exist that validate ext and do not satisfy clause 3, however, prepoints also exist that validate ext and do satisfy clause 3.

See also the overview in Remark 11.31.

Thus, this section does not alone suffice to show the existence of points, but it lays much of the technical groundwork for doing so.

11.1. We enumerate atoms, internal sets, and pairs of internal sets

Notation 11.1 will be useful:

NOTATION 11.1. Suppose ϑ is a shift permutation (Definition 2.13) and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x, x' \in \text{Set}^i$ and $\mathcal{X} \subseteq \bigcup_{i \in \mathbb{Z}} \text{Set}^i \times \text{Set}^i$ and $A \subseteq \mathbb{A}$.

Define $\vartheta^{\mathbb{Z}} \cdot a$ and $\vartheta^{\mathbb{Z}} \cdot (x, x')$ and $\vartheta^{\mathbb{Z}} \cdot \mathcal{X}$ by:

$$\begin{aligned}\vartheta^{\mathbb{Z}} \cdot a &= \{\vartheta^j(a) \mid j \in \mathbb{Z}\} \\ \vartheta^{\mathbb{Z}} \cdot (x, x') &= \{(\vartheta^j \cdot x, \vartheta^j \cdot x') \mid j \in \mathbb{Z}\} \\ \vartheta^{\mathbb{Z}} \cdot \mathcal{X} &= \bigcup \{ \vartheta^j \cdot (x, x') \mid (x, x') \in \mathcal{X}, j \in \mathbb{Z} \} \\ \vartheta^{\mathbb{Z}} \cdot A &= \bigcup \{ \vartheta^{\mathbb{Z}} \cdot a \mid a \in A \}.\end{aligned}$$

The notation ϑ^j is from Notation 2.16.

DEFINITION 11.2. We fix some shift permutation ϑ (Definition 2.13) for this Section and for the rest of this paper. One such exists by Lemma 2.14.

Recall from Definition 2.4 that $\#\mathbb{A} = \mathbb{T}_\omega$. We take advantage of this to fix some enumerations in Definitions 11.3, 11.6, and 11.8:

DEFINITION 11.3(1) Enumerate \mathbb{A}^0 as $a_{\alpha\beta}$ where $\beta \leq \alpha$. So this enumeration has the following ‘triangular’ form

$$a_{00}, a_{10}, a_{11}, a_{20}, a_{21}, a_{22}, \dots$$

Note that the subscripts above relate to the enumeration and not to levels, that is; it is not necessarily the case that $a_{\alpha\beta}$ is in \mathbb{A}^α or \mathbb{A}^β (and this does not even make sense, since α and β are not integers).

(2) Define $\mathbb{A}_{<\alpha}$ by

$$\mathbb{A}_{<\alpha} = \vartheta^{\mathbb{Z}} \cdot \{a_{\alpha'\beta'} \mid \alpha' < \alpha, \beta' \leq \alpha'\}.$$

REMARK 11.4. Definition 11.3 chooses what might seem an odd way to enumerate atoms; why not just enumerate them linearly as a_0, a_1, a_2 , and so on? The triangular arrangement makes sure that \mathcal{A}_β in Proposition 11.30 is generous.

We will mention $\mathbb{A}_{<\alpha}$ often in what follows, but perhaps its key technical moment in the proofs that follow is its role—in combination with Lemmas 10.26 and 10.27—in making Proposition 11.5 work.

PROPOSITION 11.5. For each $i \in \mathbb{Z}$ the following sets have cardinality \mathbb{T}_ω (Notation 2.2) and can be bijected:

- (1) The set \mathbb{A}^i of atoms of level i .
- (2) The set Set^i of internal sets of level i .
- (3) The set $\{\mathcal{X} \subseteq_{\text{nom}} \text{Set}^i \mid \exists \alpha. \text{supp}(\mathcal{X}) \subseteq \mathbb{A}_{<\alpha}\}$ ($\mathbb{A}_{<\alpha}$ from Definition 11.3(2)).

Proof. It follows from Definitions 2.4 and 3.1 that $\#\mathbb{A}^i = \mathbb{T}_\omega = \#\text{Set}^i$; this handles items 1 and 2 of the list. For item 3 we use Lemmas 10.26 and 10.27, noting that we do not consider *all* subsets of atoms (of which there are $\mathbb{T}_{\omega+1}$ many) but only subsets of the form $\mathbb{A}_{<\alpha}$, of which there are \mathbb{T}_ω many. \square

DEFINITION 11.6. Enumerate Set^0 as x_0, x_1, x_2, \dots in such a way that $\text{supp}(x_\alpha) \subseteq \mathbb{A}_{<\alpha}$ (Definition 11.3(2)) for every α (so in particular, $\text{supp}(x_0) = \emptyset$).

REMARK 11.7. In the enumeration of internal sets of Definition 11.6, and in the similar enumerations of Definitions 11.8 and 12.35, we do not need to assume the Axiom of Choice. If atoms are given to us with some well-ordering available²⁰ then this can be extended to syntax using standard methods. A clear survey is in [Der87].

DEFINITION 11.8. Enumerate pairs $(x, x') \in \text{Set}^0 \times \text{Set}^0$ where x and x' are such that for each α in turn we have

- (1) the elements of $\{(x, x') \in \text{Set}^0 \times \text{Set}^0 \mid \text{supp}(x) \cup \text{supp}(x') \subseteq \mathbb{A}_{<\alpha}\}$ in some arbitrary order, and then
- (2) the elements $(\text{atm}(a_{\alpha\beta}), x_\beta)_{\beta \leq \alpha}$.

The following notation will be helpful:

- Write (x_γ, x'_γ) for the tuple in the γ th position of this list.
- Also write $(\text{atm}(a), x)$ as just (a, x) ; so if the first element of the pair is an internal atom then we may not bother to write the ‘atm’.

NOTATION 11.9 (Order-type of the enumeration). Write the order type of the enumeration in Definition 11.8 as ϖ . Thus

- γ in Definition 11.8 ranges over $\gamma < \varpi$, and
- it is a fact that ϖ is the least ordinal such that $\#\varpi = \top_\omega$.

In what follows, any ordinal called γ will range over $\gamma < \varpi$ (this includes γ'). We will be explicit about ϖ where it may add clarity, and otherwise we elide it.

REMARK 11.10. We spell out an initial segment of Definition 11.8. It begins as follows:

- $\{(x, x') \in \text{Set}^0 \times \text{Set}^0 \mid \text{supp}(x) \cup \text{supp}(x') \subseteq \emptyset\}$ in some order followed by one element (a_{00}, x_0) , and then
- $\{(x, x') \in \text{Set}^0 \times \text{Set}^0 \mid \text{supp}(x) \cup \text{supp}(x') \subseteq \vartheta^{\mathbb{Z}} \cdot \{a_{00}\}\}$ in some order followed by (a_{10}, x_0) followed by (a_{11}, x_1) ,
- and so on.

Note that the enumeration of pairs in Definition 11.8 includes generously many repeats (contrast with the enumeration of atoms in Definition 11.3(1), which does not have repeats):

LEMMA 11.11. *Suppose $x, x' \in \text{Set}^0$. Then:*

- (1) *The set of γ such that $(x, x') = (x_\gamma, x'_\gamma)$ is generous.*
- (2) *For every $\gamma' < \varpi$, the set of $\gamma \geq \gamma'$ such that $(x, x') = (x_\gamma, x'_\gamma)$ is generous.*

Proof. (1) A fact of clause 1 of Definition 11.8.

- (2) From part 1 of this result, by properties of ordinals. □

We conclude with Lemma 11.12. This technical result will be useful for Proposition 11.30, but we mention it now because it illustrates how support is managed in the enumeration above:

LEMMA 11.12. *Suppose $\gamma < \varpi$ is the least index of $a_{\alpha\beta}$ in the enumeration in Definition 11.8. Suppose $0 \leq \gamma' < \gamma$ and $\mathcal{X} \subseteq \vartheta^{\mathbb{Z}} \cdot \{(x_{\gamma'}, x'_{\gamma'}) \mid \gamma' < \gamma\}$ is a subset of ϑ acting on the stages preceding γ . Then*

$$a_{\alpha\beta} \# (x_{\gamma'}, x'_{\gamma'}) \quad \text{and} \quad a_{\alpha\beta} \# \mathcal{X}.$$

²⁰To be quite precise, in Definition 2.4 we could concretely implement an atom as a pair (i, γ) where $i \in \mathbb{Z}$ and γ is an ordinal. There is no conflict here with the use of nominal techniques: our use of nominal principles does not change the fact that, externally, ZF and FM set theory are equiconsistent.

$$\begin{aligned}
p \Vdash_{AP} x=x' &\Leftrightarrow [px|_A]_P = [px'|_A]_P \\
\Phi_{PNA}(x, x') &\Leftrightarrow \forall p \in \text{PrPt}. ((p \Vdash P \wedge p \not\Vdash N) \Rightarrow (p \Vdash_{AP} x=x' \Rightarrow p \Vdash x=x'))
\end{aligned}$$

Fig. 9: Definition 11.19

Proof. The first freshness $a_{\alpha\beta}\#(x_{\gamma'}, x'_{\gamma'})$ is guaranteed by the conditions $\text{supp}(x) \cup \text{supp}(x') \subseteq \mathbb{A}_{<\alpha}$ in Definition 11.8.

The second freshness $a_{\alpha\beta}\#\mathcal{X}$ follows, using Lemma 2.53 (since the support of internal sets is finite) and using the fact that we added a prefix $\vartheta^{\mathbb{Z}}$ in the definition of $\mathbb{A}_{<\alpha}$ in Definition 11.3. \square

11.2. Constructing an extensional theory

11.2.1. We build an extensional equality theory ext . Notation 11.13 and Lemma 11.14 will be useful:

NOTATION 11.13. Suppose $i \in \mathbb{Z}$ and $\mathcal{X} \subseteq \text{Set}^i$ and $A \subseteq \mathbb{A}$. Then define $\mathcal{X}|_A$ by

$$\mathcal{X}|_A = \{x \in \mathcal{X} \mid \text{supp}(x) \subseteq A\}.$$

LEMMA 11.14. Suppose $i \in \mathbb{Z}$ and $\mathcal{X} \subseteq \text{Set}^i$ and $A \subseteq \mathbb{A}$ and suppose A is small. Then $\text{supp}(\mathcal{X}|_A) \subseteq A$.

Proof. From Lemma 2.51(2). \square

Recall the notation $[-]_P$ from Definition 10.10(3). Definition 11.15(1) generalises Definition 7.2:

DEFINITION 11.15. Suppose $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$. Suppose $A \subseteq \mathbb{A}$ is a small set of atoms. Suppose P and N are theories and $p \in \text{PrPt}$. Then:

- (1) Define $p \Vdash_{AP} x=x'$ as in Figure 9.
- (2) Define $\Phi_{PNA}(x, x')$ using \Vdash_{AP} , as in Figure 9.

REMARK 11.16. A word on the design of Definition 11.15. We want to build an extensional theory. In brief this means that if p is well-behaved with respect to that theory then

$$p \Vdash x=x' \Rightarrow p \Vdash x=x'.$$

The construction is inductive and is given in Definition 11.19. The precise statement and proof of extensionality are in Corollary 11.26.

The idea of Definition 11.19 is to saturate an equality theory so that either the left-hand side of the implication above is false or (by adding equalities) the right-hand side is true. However, the technical details are subtle, especially because we want to saturate in a very particular manner, so as to get Proposition 11.30.

It turns out that $p \Vdash x=x'$ is too strong—intuitively this is because $px = px'$ can only be decided given full knowledge of p , and during the inductive construction we only have partial knowledge of p (the precise details are in the proof Proposition 11.30, which is complex). So we work with an approximation $p \Vdash_{AP} x=x'$ that is more ‘partial’ and so more amenable to the inductive arguments we will need to make.

This approximation is designed to have two properties: $p \Vdash x=x'$ implies $p \Vdash_{AP} x=x'$ (Lemma 11.17) and, intuitively, the approximation $p \Vdash_{AP} x=x'$ should become more precise and tend to $p \Vdash x=x'$ as A and P become more detailed.

LEMMA 11.17. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$ and $A \subseteq \mathbb{A}$.

Then $p \Vdash x=x'$ implies $p \Vdash_{AP} x=x'$.

Proof. Suppose $p \Vdash x=x'$ —meaning by Definition 7.2 that $px = px'$. Then also $[px|_A]_P = [px'|_A]_P$ and by Definition 11.15 $p \Vdash_{AP} x=x'$. \square

Recall from Definition 11.2 that we fixed a shift permutation ϑ .

NOTATION 11.18. For each $\gamma < \varpi$ define A_γ by

$$A_\gamma = \bigcup \{ \text{supp}(\vartheta^j \cdot x_{\gamma'}) \mid \gamma' < \gamma, j \in \mathbb{Z} \} \cup \bigcup \{ \text{supp}(\vartheta^j \cdot x'_{\gamma'}) \mid \gamma' < \gamma, j \in \mathbb{Z} \}.$$

A less explicit but perhaps more readable rendering of Notation 11.18 is this:

$$A_\gamma = \text{supp}(\vartheta^\mathbb{Z} \cdot \{ (x_{\gamma'}, x'_{\gamma'}) \mid \gamma' < \gamma \}).$$

Recall from Definition 11.8 the enumeration of pairs (x_γ, x'_γ) for $\gamma < \varpi$:

DEFINITION 11.19. We build a sequence of pairs of small theories (P_γ, N_γ) for each $\gamma < \varpi$ using Notation 11.18 as follows:

- (1) We set:

$$P_0 = \emptyset \quad \text{and} \quad N_0 = \emptyset$$
- (2) If (P_γ, N_γ) is defined then:
 - (i) If $P_\gamma \models x_\gamma = x'_\gamma$ then set

$$P_{\gamma+1} = P_\gamma \cup \vartheta^\mathbb{Z} \cdot (x_\gamma, x'_\gamma) \quad \text{and} \quad N_{\gamma+1} = N_\gamma.$$
 Otherwise, if $(x_\gamma, x'_\gamma) \in N_\gamma$ then set²¹

$$P_{\gamma+1} = P_\gamma \quad \text{and} \quad N_{\gamma+1} = N_\gamma.$$
 - (ii) Otherwise, if $\Phi_{P_\gamma, N_\gamma, A_\gamma}(x_\gamma, x'_\gamma)$ then set

$$P_{\gamma+1} = P_\gamma \quad \text{and} \quad N_{\gamma+1} = N_\gamma \cup \vartheta^\mathbb{Z} \cdot (x_\gamma, x'_\gamma).$$
 - (iii) Otherwise, if $\neg \Phi_{P_\gamma, N_\gamma, A_\gamma}(x_\gamma, x'_\gamma)$ then set

$$P_{\gamma+1} = P_\gamma \cup \vartheta^\mathbb{Z} \cdot (x_\gamma, x'_\gamma) \quad \text{and} \quad N_{\gamma+1} = N_\gamma.$$
- (3) If λ is a nonzero limit ordinal and (P_γ, N_γ) is defined for every $\gamma < \lambda$ then set

$$P_\lambda = \bigcup_{\gamma < \lambda} P_\gamma \quad \text{and} \quad N_\lambda = \bigcup_{\gamma < \lambda} N_\gamma.$$

Finally, define

$$\text{ext} = \bigcup_{\gamma < \varpi} P_\gamma \quad \text{and} \quad \text{notext} = \bigcup_{\gamma < \varpi} N_\gamma.$$

Following the terminology of clause 3 of Definition 8.3, we can read Lemma 11.20 as noting that Definition 11.19 builds *ambiguous* theories. This will be useful in Corollary 12.13:

LEMMA 11.20. *We continue the notation of Definition 11.19.*

- (1) $\vartheta \cdot P_\gamma = P_\gamma$ and $\vartheta \cdot N_\gamma = N_\gamma$ and $\vartheta \cdot A_\gamma = A_\gamma$ for every $\gamma < \varpi$.
- (2) $\vartheta \cdot \text{ext} = \text{ext}$ and $\vartheta \cdot \text{notext} = \text{notext}$.

Following Notation 2.22 we say P_γ , N_γ , and ext and notext are all ϑ -ambiguous.

Proof. Immediate from the construction in Definition 11.19 and Notation 11.18. □

Lemma 11.21 gives an easy but useful upper bound on support; we use it in Proposition 11.30:

LEMMA 11.21. *Continuing Notation 11.18 and Definition 11.19,*

$$\text{supp}(P_\gamma) \subseteq A_\gamma \quad \text{and} \quad \text{supp}(N_\gamma) \subseteq A_\gamma \quad \text{and} \quad \text{supp}(x_\gamma) \subseteq A_\gamma$$

for every γ .

Proof. We note that by construction P_γ and N_γ are subsets of $\{(x_{\gamma'}, x'_{\gamma'}) \mid \gamma' < \gamma\}$ which is a small set. We use Lemma 2.51(2) and Subsection 2.2.2. □

²¹This can happen because our enumeration from Definition 11.8 admits repeats—and indeed, we see there are plenty of them if we consider the components for increasing supporting sets of atoms.

DEFINITION 11.22. We fix P_γ , N_γ , ext , and notext for the rest of this paper.

11.2.2. Maximality

LEMMA 11.23 (Maximality). *Suppose $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$. Then*

$$(x, x') \in \text{ext} \Leftrightarrow (x, x') \notin \text{notext}.$$

Proof. By the design of Definition 11.19, (x, x') goes into precisely one of ext or notext . \square

LEMMA 11.24. *Suppose $p \Vdash \text{ext}$ and $p \not\Vdash \text{notext}$. Suppose $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$. Then the following conditions are equivalent:*

$$p \Vdash x=x' \quad (x, x') \notin \text{notext} \quad (x, x') \in \text{ext}$$

Proof. If $p \Vdash x=x'$ then $(x, x') \notin \text{notext}$ since we assumed $p \not\Vdash \text{notext}$.

If $(x, x') \notin \text{notext}$ then $(x, x') \in \text{ext}$ by Lemma 11.23.

If $(x, x') \in \text{ext}$ then $p \Vdash x=x'$ since we assumed $p \Vdash \text{ext}$. \square

PROPOSITION 11.25. *Suppose $p \in \text{PrPt}$ and $p \Vdash \text{ext}$ and $p \not\Vdash \text{notext}$ and $x, x' \in \text{Set}^0$. Then*

$$p \Vdash x=x' \quad \text{implies} \quad p \Vdash x=x'.$$

Proof. Suppose $p \Vdash x=x'$ and $p \not\Vdash x=x'$; we derive a contradiction.

Let γ be the least ordinal in the enumeration of Definition 11.8 such that $(x, x') = (x_\gamma, x'_\gamma)$. By Lemma 11.24 $(x, x') \in \text{notext}$. Since $N_{\gamma+1} \subseteq \text{notext}$ it must be that (x, x') is added to N_γ by clause 2ii of Definition 11.19. Thus $\Phi_{P_\gamma, N_\gamma, A_\gamma}(x, x')$ must hold.

Now $p \Vdash \text{ext}$ and $p \not\Vdash \text{notext}$ so $p \Vdash P_\gamma$ and $p \not\Vdash N_\gamma$, and it follows from $\Phi_{P_\gamma, N_\gamma, A_\gamma}(x, x')$ that $p \Vdash_{A_\gamma P_\gamma} x=x' \Rightarrow p \Vdash x=x'$. We assumed $p \Vdash x=x'$ and by Lemma 11.17 $p \Vdash_{A_\gamma P_\gamma} x=x'$, so that $p \Vdash x=x'$. This contradicts our assumption that $p \not\Vdash x=x'$. \square

In Definition 11.19 we gave ext a name (' ext ') that suggests extensionality. This is justified by Corollary 11.26:

COROLLARY 11.26. *If $p \in \text{PrPt}$ is ϑ -ambiguous then $p \Vdash \text{ext}$ and $p \not\Vdash \text{notext}$ implies p is extensional, in the sense that p satisfies clause 2 of Definition 8.3: for every $i \in \mathbb{Z}$ and $x, x' \in \text{Set}^i$*

$$p \Vdash x=x' \Rightarrow p \Vdash x=x'.$$

Proof. Suppose $i \in \mathbb{Z}$ and $p \Vdash x=x'$. Note that $\vartheta^{-i} \cdot x, \vartheta^{-i} \cdot x' \in \text{Set}^0$. By assumption $\vartheta \cdot p = p$ so using Theorem 2.31 $p \Vdash \vartheta^{-i} \cdot x = \vartheta^{-i} \cdot x'$. Thus by Proposition 11.25 $p \Vdash \vartheta^{-i} \cdot x = \vartheta^{-i} \cdot x'$ and using Theorem 2.31 again, $p \Vdash x=x'$ as required. \square

11.2.3. Deductive closure and consistency

LEMMA 11.27(1) $\text{ext} = [\text{ext}]_{\text{eq}}$.

(2) $[P_\gamma]_{\text{eq}} \cap N_\gamma = \emptyset$ for every $\gamma < \omega$, and $[\text{ext}]_{\text{eq}} \cap \text{notext} = \emptyset$.

Proof. (1) We have $\text{ext} \subseteq [\text{ext}]_{\text{eq}}$ by Lemma 10.11(1).

For the reverse inclusion, note by Lemma 11.20(2) that $\vartheta \cdot \text{ext} = \text{ext}$ so by Theorem 2.31(2) $\vartheta \cdot [\text{ext}]_{\text{eq}} = [\text{ext}]_{\text{eq}}$. Thus it suffices to prove that $(x, x') \in [\text{ext}]_{\text{eq}}$ implies $(x, x') \in \text{ext}$ for $(x, x') \in \text{Set}^0 \times \text{Set}^0$ —that is, we only need to consider level 0.

So consider $(x, x') \in \text{Set}^0 \times \text{Set}^0$. Recalling the enumeration of $\text{Set}^0 \times \text{Set}^0$ from Definition 11.8, let γ be least such that the following two conditions hold:

- (a) $(x, x') \in [P_\gamma]_{\text{eq}}$, and
- (b) $(x_\gamma, x'_\gamma) = (x, x')$.

The first condition is satisfiable since by Lemma 10.11(3) $[\text{ext}]_{\text{eq}} = \bigcup_{\gamma} [P_{\gamma}]_{\text{eq}}$. The second condition is satisfiable by Lemma 11.11(2).

It follows from clause 2i in the construction of ext in Definition 11.19 that $(x_{\gamma}, x'_{\gamma}) \in P_{\gamma+1}$, and so that $(x, x') \in \text{ext}$ as required.

(2) Part 2 follows combining part 1 of this result with Lemma 11.23. \square

REMARK 11.28. We have not extended Corollary 10.22 and proved that $(\text{empt}^i, \text{set}^i) \notin \text{ext}$. Our construction does not guarantee this. We could (for a price in proof-complexity); we do not because it does not matter.²²

Our interest in ext is that it should satisfy Proposition 11.25, that $p \Vdash x=x'$ implies $p \Vdash x=x'$ for every $(x, x') \in \text{ext}$. From Lemma 6.12 $p \not\Vdash \text{empt}^i = \text{set}^i$, so this implication is guaranteed regardless of whether $(\text{empt}^i, \text{set}^i) \in \text{ext}$, or not.

Put another way, in our examination of $\text{herb}(\text{ext})$ in Subsection 11.3, ext governs what happens ‘to the left of \in ’. Behaviour ‘to the right of \in ’ is a distinct issue which is handled later on, by a different method, in Definition 12.37.

11.2.4. *Generous naming in ext.* We show that the theory ext from Definition 11.19 generously names internal sets, in a certain formal sense—and so by Corollary 12.51 it generates a point.

Definition 11.29 is clearly related to Definitions 8.3(1) and 11.35:

DEFINITION 11.29. Suppose T is a theory.

(1) Say T **generously names internal sets** when

$$\forall i \in \mathbb{Z}. \forall x \in \text{Set}^i. \exists a \in \mathbb{A}^i. T \models a = x.$$

(2) Say T **generously names internal atoms** when

$$\forall i \in \mathbb{Z}. \forall a \in \mathbb{A}^i. \exists a' \in \mathbb{A}^i. T \models a = a'.$$

PROPOSITION 11.30(1) ext generously names internal sets (Definition 11.29).

(2) ext generously names internal atoms.

Proof. It is clear from Definition 11.29 that part 2 follows from part 1. For part 1, we need only consider internal sets at level 0 (that is, $x \in \text{Set}^0$), and the result follows for other levels by Lemma 11.20(2).

So choose $x \in \text{Set}^0$ and let β be the index of x in the enumeration of Definition 11.6, so that $x = x_{\beta}$.

Recall from Definition 11.8 the enumeration of pairs of internal sets; this enumeration includes $(a_{\alpha\beta}, x_{\beta})$ for every α such that $\beta \leq \alpha$. It is a fact that there are T_{ω} many such α , so the set

$$\mathcal{A}_{\beta} = \{a_{\alpha\beta} \in \mathbb{A}^0 \mid \beta \leq \alpha\}$$

is generous (Notation 2.6).

Choose any $a_{\alpha\beta} \in \mathcal{A}_{\beta}$ and let γ be the least index of $(a_{\alpha\beta}, x_{\beta})$ in the enumeration of Definition 11.8. It suffices now to prove that clause 2 of Definition 11.19 adds $(a_{\alpha\beta}, x_{\beta})$ to P_{γ} (and not to N_{γ}).

For brevity we write x for x_{β} . We check which clause in Definition 11.19 is activated by $(a_{\alpha\beta}, x)$ at stage γ :

(i) We consider clause 2i of Definition 11.19.

By construction P_{γ} is small (Definition 10.1). Thus by Lemma 11.12 and minimality of γ we have $a_{\alpha\beta} \# P_{\gamma}$. It follows using Lemma 10.15 that $(a_{\alpha\beta}, x) \notin [P_{\gamma}]_{\text{eq}}$.

Also using Lemma 11.12 it follows that $(a_{\alpha\beta}, x) \notin N_{\gamma}$.

Therefore clause 2i is not activated.

²²In case this matters in future work we sketch how the constructions would change: we take $N_0 = \vartheta^{\mathbb{Z}} \cdot (\text{empt}^0, \text{set}^0)$ in Definition 11.19(1), use Corollary 10.22, and update the proof of Lemma 11.23 accordingly.

- (ii) We consider clause 2ii of Definition 11.19.

We will prove that this clause is not activated; it suffices to exhibit a $p' \in \text{PrPt}$ such that $p' \Vdash P_\gamma$ and $p' \not\Vdash N_\gamma$ and $p' \Vdash_{A_\gamma P_\gamma} a_{\alpha\beta} = x$ and $\neg(p' \Vdash a_{\alpha\beta} = x)$.

We first construct an intermediate prepoint $p \in \text{PrPt}$ as follows:

- (a) We set $pn = \emptyset$ for every $n \in A_\gamma$ (A_γ is from Notation 11.18).
- (b) We let p name (in the sense of Notation 10.17) every \mathcal{X} such that $\mathcal{X} \Vdash P_\gamma$ and $\text{supp}(\mathcal{X}) \subseteq A_\gamma$. By Lemma 10.27 we can do this using a set \mathcal{B} of at most $2^{\#A_\gamma}$ many atoms, where we select $\mathcal{B} \subseteq \mathbb{A} \setminus A_\gamma$.
- (c) Take a disjoint $\mathcal{B}' \subseteq \mathbb{A} \setminus (A_\gamma \cup \mathcal{B})$ of the same cardinality as \mathcal{B} , so that $b' \in \mathcal{B}'$ bijects with $b \in \mathcal{B}$.
For each $b' \in \mathcal{B}'$ set $pb' = [b]_{P_\gamma}$ (Definition 10.10).²³
- (d) For the \top_ω remaining atoms $n \in \mathbb{A} \setminus (A_\gamma \cup \mathcal{B} \cup \mathcal{B}')$ we set $pn = \emptyset$.

We note that $p \Vdash P_\gamma$ and $p \not\Vdash N_\gamma$, as follows:

— *Proof that $p \Vdash P_\gamma$.*

By Lemma 10.12(3) $\emptyset \Vdash P_\gamma$.

By assumption $pb \Vdash P_\gamma$ for every $b \in \mathcal{B}$.

By Lemma 10.12(1) (noting that $P_\gamma \subseteq \text{ext}$) $[b']_{\text{ext}} \Vdash P_\gamma$ for every $b' \in \mathcal{B}'$.

It follows that by construction $p \Vdash P_\gamma$.

— *Proof that $p \not\Vdash N_\gamma$.*

Consider an arbitrary $(y, y') \in N_\gamma$. By Lemmas 10.14 and 11.21, $\text{supp}(y) \subseteq A_\gamma$, so that $\text{supp}([y]_{P_\gamma}) \subseteq A_\gamma$ by Lemma 11.21 and Theorem 2.31(3). Also $[y]_{P_\gamma} \Vdash P_\gamma$ by Lemma 10.12(1). It follows that $[y]_{P_\gamma}$ is one of the sets \mathcal{X} named in p by some atom $b \in \mathcal{B}$.

Now by Lemma 11.27(2) $[P_\gamma]_{\text{eq}} \cap N_\gamma = \emptyset$, so that $(y, y') \notin [P_\gamma]_{\text{eq}}$ and so (unpacking Definition 10.10) $y' \notin [y]_{P_\gamma}$. Since $[y]_{P_\gamma}$ was named in p , it follows that $p \not\Vdash y = y'$.

Finally, $(y, y') \in N_\gamma$ was arbitrary, so $p \not\Vdash N_\gamma$.

We now (recalling Notation 11.13 for $-|_{A_\gamma}$) define

$$\mathcal{X} = [px|_{A_\gamma}]_{P_\gamma}.$$

We note by Lemma 10.12(2) that $[\mathcal{X}]_{P_\gamma} = \mathcal{X}$. Then

$$\mathcal{X}|_{A_\gamma} \stackrel{\text{L10.11(1)}}{\subseteq} [\mathcal{X}|_{A_\gamma}]_{P_\gamma} \stackrel{\text{L10.11(2)}}{\subseteq} [\mathcal{X}]_{P_\gamma} \stackrel{\text{L10.12(2)}}{=} \mathcal{X}.$$

By Theorem 2.31(3) and Lemma 11.14 $\text{supp}(\mathcal{X}) \subseteq A_\gamma$.

It follows by clause iib above in the construction of $p \in \text{PrPt}$ that there exists a $b \in \mathcal{B}$ with $b \# A_\gamma$ and $pb = \mathcal{X}$, and thus p names \mathcal{X} .

Now define

$$p' = (a_{\alpha\beta} b) \cdot p.$$

We chose $b, a_{\alpha\beta} \notin A_\gamma$ so by Lemma 11.21 $b, a_{\alpha\beta} \# P_\gamma, N_\gamma, x$ and by Corollary 2.28 $(a_{\alpha\beta} b) \cdot P_\gamma = P_\gamma$ and $(a_{\alpha\beta} b) \cdot N_\gamma = N_\gamma$. Then using Theorem 2.31

$$p' \Vdash P_\gamma \quad p' \not\Vdash N_\gamma \quad \text{and} \quad [p' a_{\alpha\beta} |_{A_\gamma}]_{P_\gamma} = [p' x |_{A_\gamma}]_{P_\gamma} \text{ equivalently } p' \Vdash_{A_\gamma P_\gamma} a_{\alpha\beta} = x$$

Also we should check that

$$p' \not\Vdash a_{\alpha\beta} = x, \quad \text{that is,} \quad p \not\Vdash b = x.$$

This follows noting that:

- We have $b \in pb' = [b]_{P_\gamma}$ from clause iic above, in the construction of $p \in \text{PrPt}$, since $b \in [b]_{P_\gamma}$.
- We have $x \notin pb' = [b]_{P_\gamma}$ from Corollary 10.16, since it follows from clause iib above that $b \# x$, and also $b \notin A_\gamma$ so by Lemma 11.21 $b \# P_\gamma$.

Thus clause 2ii is not activated.

²³We do this to block $p \Vdash b = x$, below.

Therefore clause 2iii of Definition 11.19 is the one used at stage γ , and $(a_{\alpha\beta}, x_\beta) \in P_\gamma$ as required. \square

11.3. Properties of the Herbrand prepoint for ext

Recall the *Herbrand prepoint* $\text{herb}(-)$ from Definition 10.18 and ext from Definition 11.19.

REMARK 11.31. Could it be that $\text{herb}(\text{ext})$ is a point, so that we can use Corollary 9.30 to deduce the consistency of TST+ and thus the consistency of NF? By Definition 8.3(4) a point is a prepoint that is extensional, ambiguous, and generously names every internal set. We have proved results to the effect that ext is extensional, ambiguous, and generously names every internal set: see Corollary 11.26, Lemma 11.20(2), and Proposition 11.30(1). So this seems promising.

We shall see that $\text{herb}(\text{ext})$ is extensional, ambiguous, and generously names every internal *atom*—see Proposition 11.36—but it need not generously name every internal set. So $\text{herb}(\text{ext})$ is not quite a point, however, we will use it in Section 12 to construct something that is a point.

11.3.1. A simple property

LEMMA 11.32(1) $\text{herb}(\text{ext}) \Vdash \text{ext}$.

(2) $\text{herb}(\text{ext}) \not\Vdash \text{not ext}$.

(3) $\vartheta \cdot \text{herb}(\text{ext}) = \text{herb}(\text{ext})$.

Proof. (1) Immediate from Lemma 10.20(2).

(2) Consider $i \in \mathbb{Z}$ and $u, u' \in \text{Set}^i$ and $(u, u') \in \text{not ext}$, so that by Lemma 11.23 also $\text{ext} \Vdash^{\text{sa}} u = u'$.

By Proposition 11.30(1) ext generously names u and u' , so by Definition 11.29 there exist $a, a' \in \mathbb{A}^i$ such that $\text{ext} \Vdash^{\text{sa}} a = u$ and $\text{ext} \Vdash^{\text{sa}} a' = u'$. Also $\text{ext} \Vdash^{\text{sa}} a = a'$ since we assumed $\text{ext} \Vdash^{\text{sa}} u = u'$. Thus $u \in [a]_{\text{ext}}$ and $u' \notin [a]_{\text{ext}}$, so that by Definition 10.18 $u \in \text{herb}(\text{ext})(\vartheta(a))$ and $u' \notin \text{herb}(\text{ext})(\vartheta(a))$. By Figure 1 ($\sigma\mathbf{a}$) $\text{herb}(\text{ext}) \models c[c \mapsto u] \in \vartheta(a)$ and $\text{herb}(\text{ext}) \not\models c[c \mapsto u'] \in \vartheta(a)$ where $c \in \mathbb{A}^i$, and by Definition 7.2 $\text{herb}(\text{ext}) \not\models u = u'$ as required.

(3) By Lemma 11.20(2) $\vartheta \cdot \text{ext} = \text{ext}$ so by Lemma 10.20(1) $\vartheta \cdot \text{herb}(\text{ext}) = \text{herb}(\text{ext})$. \square

11.3.2. Naming atoms

LEMMA 11.33. Suppose $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$. Then

$$\text{ext} \Vdash^{\text{sa}} a = a' \text{ implies } \text{herb}(\text{ext}) \models a = a'.$$

Proof. Suppose $(a, a') \in \text{ext}$. It follows from Definition 10.10 that $[a]_{\text{ext}} = [a']_{\text{ext}}$ and so that $\text{herb}(\text{ext})(\vartheta(a)) = \text{herb}(\text{ext})(\vartheta(a'))$. We apply ϑ^{-1} to both sides of this equality and by Theorem 2.31 conclude that $\text{herb}(\vartheta^{-1} \cdot \text{ext})(a) = \text{herb}(\vartheta^{-1} \cdot \text{ext})(a')$. By Lemma 11.20 $\vartheta \cdot \text{ext} = \text{ext}$ and it follows that $\text{herb}(\text{ext})(a) = \text{herb}(\text{ext})(a')$ as required. \square

LEMMA 11.34. Suppose $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$. Suppose $\text{herb}(\text{ext}) \models a = a'$. Then we have:

(1) $\text{herb}(\text{ext}) \models a = a'$.

(2) For every $X \in \text{Pred}$ and $a'' \in \mathbb{A}^i$,

$$\text{herb}(\text{ext}) \models X[a'' \mapsto a] \text{ if and only if } \text{herb}(\text{ext}) \models X[a'' \mapsto a'].$$

Proof. Part 1 follows from Corollary 11.26, since by Lemma 11.32 $\text{herb}(\text{ext}) \Vdash \text{ext}$ and $\text{herb}(\text{ext}) \not\Vdash \text{not ext}$ and $\text{herb}(\text{ext})$ is ϑ -ambiguous.

Part 2 follows by Proposition 7.6. \square

Definition 11.35 continues the notation of Definition 8.1:

DEFINITION 11.35. Say that $p \in \text{PrPt}$ **generously names internal atoms** when it generously names $\text{atm}(a')$ for every atom $a' \in \mathbb{A}$.

Unpacking Definition 8.1, this means that for every $a' \in \mathbb{A}$ and every $a \in \mathbb{A}^{\text{level}(a')}$ and $X \in \text{Pred}$,

$$\exists a'' \in \mathbb{A}^{\text{level}(a')}. (p \models (a'' a) \cdot X \Leftrightarrow p \models X[a \mapsto a']).$$

PROPOSITION 11.36. $\text{herb}(\text{ext})$ generously names internal atoms (Definition 11.35).

Proof. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$. By Proposition 11.30(2) $\text{ext} \models^{\text{eq}} a = a'$ for generously many a' , so by Lemma 11.33 $\text{herb}(\text{ext})(a) = \text{herb}(\text{ext})(a')$ for generously many a' . We use Lemmas 11.34(2) and 4.17. \square

REMARK 11.37. $\text{herb}(\text{ext})$ generously names internal atoms, but it does not generously name internal sets. Yet in Proposition 11.30 we proved that ext generously names internal sets and atoms. Why the difference? We give some intuition:

Suppose $(x = x') \in \text{ext}$. Then it is a fact of the construction in Definition 10.18 that $\text{herb}(\text{ext})$ satisfies $\text{herb}(\text{ext}) \models z[a \mapsto x] \in c \Leftrightarrow z[a \mapsto x'] \in c$ for every c (choosing levels appropriately). See Lemma 11.32(2).

However, there is no clear reason that $\text{herb}(\text{ext}) \models y \in x \Leftrightarrow y \in x'$ should always hold. (We do know this if x and x' are atoms by Lemma 11.33; and we know from Corollary ?? that $x = \text{empt}$ and $x' = \text{set}^i$ is not possible.)

Remarkably, it will turn out that we can leverage what we have to build a point. The technical details follow. See also Remark 11.39.

11.3.3. Extensionality, using internal predicates

PROPOSITION 11.38. For every $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$ and $b \in \mathbb{A}^{i-1}$ and $c \in \mathbb{A}^{i+1}$,

$$\text{herb}(\text{ext}) \models \forall a. \forall a'. (\forall b. (b \in a \Leftrightarrow b \in a')) \Rightarrow \forall c. (a \in c \Leftrightarrow a' \in c).$$

Proof. By Lemma 11.32 $\text{herb}(\text{ext}) \Vdash \text{ext}$ and $\text{herb}(\text{ext}) \nVdash \text{not ext}$ and $\text{herb}(\text{ext})$ is ϑ -ambiguous. It follows by Corollary 11.26 that $\text{herb}(\text{ext}) \Vdash u = u'$ implies $\text{herb}(\text{ext}) \models u = u'$, for any u and u' of the same level.

By Figure 3 (**modall**) and Lemma 5.9(1&2)

$$\begin{aligned} \text{herb}(\text{ext}) \models \forall a. \forall a'. (\forall b. (b \in a \Leftrightarrow b \in a')) \Rightarrow \forall c. (a \in c \Leftrightarrow a' \in c) \\ \text{when } \forall a, a'. (\forall b. \text{herb}(\text{ext}) \models b \in a \Leftrightarrow \text{herb}(\text{ext}) \models b \in a') \Rightarrow \\ \forall c. (\text{herb}(\text{ext}) \models a \in c \Leftrightarrow \text{herb}(\text{ext}) \models a' \in c). \end{aligned}$$

Using Proposition 11.30(1) and Lemma 2.11(5)—this step is important; see Remark 11.39 below—we can simplify this to

$$\forall a, a'. (\forall y. \text{herb}(\text{ext}) \models y \in a \Leftrightarrow \text{herb}(\text{ext}) \models y \in a') \Rightarrow \forall c. (\text{herb}(\text{ext}) \models a \in c \Leftrightarrow \text{herb}(\text{ext}) \models a' \in c).$$

Using Definition 7.2 we can simplify this further to

$$\forall a, a'. (\text{herb}(\text{ext}) \Vdash a = a') \Rightarrow \forall c. (\text{herb}(\text{ext}) \models a \in c \Leftrightarrow \text{herb}(\text{ext}) \models a' \in c).$$

Now suppose $\text{herb}(\text{ext}) \Vdash a = a'$. By Lemma 11.34(2) $\text{herb}(\text{ext}) \models a \in c \Leftrightarrow \text{herb}(\text{ext}) \models a' \in c$ for all $c \in \mathbb{A}^{i+1}$, and therefore for cosmall many c . The result follows. \square

REMARK 11.39. The step noted above is important. We know $\text{herb}(\text{ext}) \nVdash \text{ext}$. Intuitively, this implies that, at $\text{herb}(\text{ext})$, the \forall -quantified atom b has the meaning of ‘any y ’ so long as it is to the left of \in . Inside the scope of $\forall b$, b does indeed always appear to the left of \in . This allows us to convert

$$\forall b. \text{herb}(\text{ext}) \models b \in a \Leftrightarrow \text{herb}(\text{ext}) \models b \in a' \quad \text{into} \quad \forall y. \text{herb}(\text{ext}) \models y \in a \Leftrightarrow \text{herb}(\text{ext}) \models y \in a'$$

and so into $\text{herb}(\text{ext}) \Vdash a = a'$.

We cannot use the same trick for c , because c appears to the right of \in . This, and other issues, will be handled in Section 12. That Section depends on the existence of $\text{herb}(\text{ext})$, and in particular on Proposition 11.38. If it helps the reader, it may be useful to think of this Section as “turning the b into a y ”, and Section 12 as “turning the c into a z ”.

$$\begin{aligned}
\vartheta\text{-AMBIG} &= \{X \Leftrightarrow \vartheta \cdot X \mid X \in \text{Pred}\} \\
\text{EXTEN} &= \{\forall a. \forall a'. (\forall b. (b \in a \Leftrightarrow b \in a')) \Rightarrow (\forall c. (a \in c \Leftrightarrow a' \in c)) \mid i \in \mathbb{Z}, a, a' \in \mathbb{A}^i, b \in \mathbb{A}^{i-1}, c \in \mathbb{A}^{i+1}\} \\
\text{ATOMI} &= \{X[a \mapsto u] \Leftrightarrow X[a \mapsto [b](b \in u)] \mid X \in \text{Pred}, i \in \mathbb{Z}, a \in \mathbb{A}^i, u \in \text{Set}^i, b \in \mathbb{A}^{i-1}\} \\
\Theta &= \vartheta\text{-AMBIG} \cup \text{EXTEN} \cup \text{ATOMI}
\end{aligned}$$

Fig. 10: Three sets of internal predicates

11.3.4. Three sets of internal predicates. Recall ϑ the shift permutation that we fixed in Definition 11.2:

DEFINITION 11.40. Define sets of internal predicates $\vartheta\text{-AMBIG}$, EXTEN , ATOMI , and Θ as in Figure 10.

REMARK 11.41. The main result of this Subsection is Proposition 11.45, that $\text{herb}(\text{ext}) \models \Theta$. This is important because it will help us later, as follows:

- (1) $\vartheta\text{-AMBIG}$ gives us Lemma 12.44.
- (2) EXTEN gives us Lemma 12.50.
- (3) ATOMI reduces case 2 in the proof of Lemma 12.45, to case 1. This is a final echo of our syntactic treatment of internal atoms, as discussed in Remark 5.5(4).

Lemma 11.42 will be useful:

LEMMA 11.42. Suppose $p \in \text{PrPt}$. Then $p \models \vartheta\text{-AMBIG}$ if and only if p is ϑ -ambiguous (meaning that $\vartheta \cdot p = p$).

Proof. Suppose $p \models \vartheta\text{-AMBIG}$. We reason as follows:

$$\begin{aligned}
a \circ y \in p &\Leftrightarrow p \models y \in a && \text{Figure 3(modelt)} \\
&\Leftrightarrow p \models \vartheta \cdot y \in \vartheta(a) && \text{Assumption} \\
&\Leftrightarrow \vartheta(a) \circ \vartheta \cdot y \in p && \text{Figure 3(modelt)}
\end{aligned}$$

It follows that $\vartheta \cdot p = p$.

Conversely if $\vartheta \cdot p = p$ then we reason as follows:

$$\begin{aligned}
p \models X &\Leftrightarrow \vartheta \cdot p \models \vartheta \cdot X && \text{Theorem 2.31} \\
&\Leftrightarrow p \models \vartheta \cdot X && \vartheta \cdot p = p
\end{aligned}$$

It follows by Lemma 5.9(2) that $p \models \vartheta\text{-AMBIG}$. □

LEMMA 11.43. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $u \in \text{Set}^i$ and $b \in \mathbb{A}^{i-1}$. Then:

- (1) $p \Vdash u = [b]\text{elt}(\text{atm}(b), u)$.
- (2) $\text{herb}(\text{ext}) \Vdash u = [b]\text{elt}(\text{atm}(b), u)$ and $\text{herb}(\text{ext}) \models u = [b]\text{elt}(\text{atm}(b), u)$.
- (3) $\text{herb}(\text{ext}) \models \text{ATOMI}$.

Proof. (1) We unpack \Vdash from Definition 7.2 and note that this is just Lemma 6.9.

- (2) $\text{herb}(\text{ext})$ is a prepoint so the \Vdash is just a special case of part 1. For the \models we use Lemma 11.32 and Corollary 11.26.
- (3) By part 2 of this result and Proposition 7.6. □

REMARK 11.44. Lemma 11.43 combines no fewer than three entailment symbols: \Vdash , \models , and \models . For the reader's convenience we take a moment to recall them and where they come from:

- \models is *validity* from Definition 5.4. Intuitively, $p \models X$ when X is indeed true (at p), or topologically: when p is an element of X viewed as an open set.
- \Vdash and \models are from Definition 7.2:

- $p \Vdash u=u'$ when $p \models y \in u \Leftrightarrow p \models y \in u'$. So intuitively p believes that u and u' are interchangeable, to the right of \in .
- $p \Vdash u=u'$ when $p \models z[c \mapsto u] \in a \Leftrightarrow p \models z[c \mapsto u'] \in a$. So intuitively p believes that u and u' are intersubstitutable, to the left of \in .

PROPOSITION 11.45(1) $herb(\text{ext}) \models \vartheta\text{-AMBIG}$.

(2) $herb(\text{ext}) \models \text{EXTEN}$.

(3) $herb(\text{ext}) \models \text{ATOMI}$.

(4) As a corollary, $herb(\text{ext}) \models \Theta$.

Proof. (1) From Lemmas 11.32(3) and 11.42, $herb(\text{ext}) \models \vartheta\text{-AMBIG}$.

(2) By Proposition 11.38 $herb(\text{ext}) \models \text{EXTEN}$.

(3) From Lemma 11.43(3).

(4) Thus $herb(\text{ext}) \models \Theta$. □

REMARK 11.46. As discussed in Remark 11.31, Proposition 11.45 says intuitively that $herb(\text{ext})$ is not quite a point. In Section 12 we will use $herb(\text{ext})$ to build a point. Some technical machinery is required first: the key construction is in Definition 12.37.

12. EXISTENCE OF A POINT

We are now ready to construct a point. A few words first on proofs that do not work, to help the reader understand the forces shaping the proof that does work.

- (1) The usual way to build a point is to saturate a consistent (for some suitable definition of ‘consistent’) set of predicates to make a maximally consistent set of predicates. We add predicates one at a time until we can do so no longer, and then we stop. If some constraints are needed—in our case these are the three conditions of Definition 8.3—then we make sure that every time we add a predicate we preserve those conditions, and we note that the conditions are preserved under unions of ascending chains of sets of predicates that satisfy the conditions.

This will not work: adding a predicate may break ϑ -ambiguity (condition 3 of Definition 8.3).

- (2) Another approach is this: we just take the syntactic model $herb(\text{ext})$, which we know by Proposition 11.45 has excellent properties.

This will not work: $herb(\text{ext})$ generously names internal atoms by Proposition 11.36, but condition 1 of Definition 8.3 requires it to name every internal set, and this is false.

- (3) Perhaps, we can apply the \neg -action to $herb(\text{ext})$ \top_ω many times, which by Lemma 12.24 will force it to generously name every internal set.

This also will not work: the necessary \neg -action would be large, and Lemma 12.24 works only for a small action (one substituting a small number of atoms).

So we take a hybrid of all three approaches above: First, we develop a notion of entailment weak enough to be sound (Theorem 12.11) and just strong enough to satisfy Cut-admissibility (Proposition 12.16).

Interestingly, for the proof of Cut-admissibility to work we require atoms-for-atoms substitutions in the forall-left intro rule ($\forall\text{allL}$) in Figure 11, and in the proof of soundness (Theorem 12.11) this translates to a condition that a prepoint generously name internal atoms. Proposition 11.36, which seemed too weak when mentioned above, is *just* strong enough for the proofs to squeeze through at this point.

Then we create a maximally consistent set of predicates in Definition 12.37. This construction uses a small \neg -action as discussed above for all small stages; at the final transfinite induction (clause 5 of Definition 12.37) we must abandon the \neg -action (because it becomes ‘too large’)—but we can still retain the set of predicates.

We now have a maximally consistent set of predicates, which we write $\text{maxfilt}(\Theta)$. After non-trivial but ultimately routine technical calculations and verifications on $\text{maxfilt}(\Theta)$ —the most inter-

$\frac{\Gamma, \mathcal{X} \vdash_{\text{pd}} \Delta}{\Gamma, \text{and}(\mathcal{X}) \vdash_{\text{pd}} \Delta} (\text{andL})$	$\frac{\Gamma \vdash_{\text{pd}} X, \Delta \text{ for every } X \in \mathcal{X}}{\Gamma \vdash_{\text{pd}} \text{and}(\mathcal{X}), \Delta} (\text{andR})$
$\frac{\Gamma \vdash_{\text{pd}} X, \Delta}{\Gamma, \text{neg}(X) \vdash_{\text{pd}} \Delta} (\text{negL})$	$\frac{\Gamma, X \vdash_{\text{pd}} \Delta}{\Gamma \vdash_{\text{pd}} \text{neg}(X), \Delta} (\text{negR})$
$\frac{\Gamma, X[a \mapsto a'] \vdash_{\text{pd}} \Delta}{\Gamma, \text{all}[a]X \vdash_{\text{pd}} \Delta} (\text{allL})$	$\frac{\forall a'. (\Gamma \vdash_{\text{pd}} (a' a) \cdot X, \Delta)}{\Gamma \vdash_{\text{pd}} \text{all}[a]X, \Delta} (\text{allR})$
$\frac{}{\Gamma, X \vdash_{\text{pd}} X, \Delta} (\text{Ax})$	$\frac{\Gamma, X \vdash_{\text{pd}} \Delta \quad \Gamma \vdash_{\text{pd}} X, \Delta}{\Gamma \vdash_{\text{pd}} \Delta} (\text{Cut})$

Fig. 11: Entailment \vdash_{pd} for Definition 12.1

esting is probably Lemma 12.45—it is not hard to extract a point from $\text{maxfilt}(\Theta)$ in the sense of Definition 8.3. This is $G(\text{maxfilt}(\Theta))$ in Corollary 12.51, and thus we are done.

12.1. An entailment relation

12.1.1. Basic definitions and lemmas

DEFINITION 12.1. A **context** is a finite set of internal predicates. Γ and Δ will range over contexts.

In the case of sets of internal predicates, we may drop singleton sets brackets and write comma for sets union; thus for instance Γ, X means $\Gamma \cup \{X\}$.

Define an **entailment** relation $\Gamma \vdash_{\text{pd}} \Delta$ inductively by the rules in Figure 11.

REMARK 12.2. The rules in Figure 11 may seem unsurprising but subtlety goes into the design of (allL).

(allL) has an atom-for-atom substitution $[a \mapsto a']$. This is both weaker and stronger than expected: *weaker* because $[a \mapsto u]$ would be more usual in a forall left intro rule, and *stronger* because Figure 3 (modall) would suggest we use a \exists quantifier and a permutation here, rather than an existential and a substitution.

Using $[a \mapsto u]$ is too strong: we would not be able to prove soundness in Theorem 12.11. A generous quantifier and a permutation is too weak: we would lose Lemma 12.6.

So Figure 11 is not as simple as it seems, and seems to be striking quite a delicate balance.

Definition 12.3 extends Definition 12.1:

DEFINITION 12.3. If $\mathcal{C}, \mathcal{D} \subseteq \text{Pred}$ are sets of internal predicates then write $\mathcal{C} \vdash_{\text{pd}} \mathcal{D}$ when there exist contexts $\Gamma \subseteq \mathcal{C}$ and $\Delta \subseteq \mathcal{D}$ (that is, finite subsets of \mathcal{C} and \mathcal{D}) such that $\Gamma \vdash_{\text{pd}} \Delta$ is derivable.

Following Definition 12.1 we may write comma for sets union of internal predicates, thus for instance \mathcal{C}, \mathcal{D} means $\mathcal{C} \cup \mathcal{D}$.

NOTATION 12.4. Henceforth we may write true and false from Example 3.9 as \top and \perp respectively.

NOTATION 12.5— Call a set $\mathcal{C} \subseteq \text{Pred}$ of internal predicates **consistent** when $\mathcal{C} \not\vdash_{\text{pd}} \perp$.

— Call \mathcal{C} **maximally consistent** when it is consistent and for any consistent $\mathcal{C}' \subseteq \text{Pred}$ if $\mathcal{C} \subseteq \mathcal{C}'$ then $\mathcal{C} = \mathcal{C}'$.

— Call \mathcal{C} **deductively closed** when $\mathcal{C} \vdash_{\text{pd}} X$ implies $X \in \mathcal{C}$.

Lemmas 12.6, 12.7, and 12.8 have standard proofs and will be useful later (in Lemmas 12.47 and 12.43 and Proposition 12.41 respectively). We mention them now:

LEMMA 12.6. Suppose Γ and Δ are contexts and $X \in \text{Pred}$ is an internal predicate and suppose $i \in \mathbb{Z}$ and $a, n \in \mathbb{A}^i$, where n is not necessarily distinct from a . Then

$$\Gamma, \forall a. X \Vdash X[a \mapsto n], \Delta \quad \text{is derivable.}$$

Proof. Using (allL) and (Ax) . □

LEMMA 12.7. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $X \in \text{Pred}$. Then $X \Vdash \forall a. X$ and $\forall a. X \Vdash X$.

Proof. By standard reasoning using the rules in Figure 11 and Lemma 4.16. □

LEMMA 12.8. Suppose $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \dots$ is an infinite ascending chain of sets of predicates. Then if every \mathcal{C}_γ is consistent, then so is their union.

Proof. By Definition 12.3 $\bigcup \mathcal{C}_\gamma \Vdash \perp$ implies there exists a finite context $\Gamma \subseteq \bigcup \mathcal{C}_\gamma$ such that $\Gamma \Vdash \perp$. Thus there must be some index γ such that $\Gamma \subseteq \mathcal{C}_\gamma$ and so $\mathcal{C}_\gamma \Vdash \perp$, contradicting our assumption that \mathcal{C}_γ is consistent. □

12.1.2. *Soundness, and a corollary of soundness.* Definition 12.9 extends the validity relation $p \models X$ from Definition 5.4:

DEFINITION 12.9. Suppose $\mathcal{C}, \mathcal{D} \subseteq \text{Pred}$ are sets of internal predicates. Suppose $p \in \text{PrPt}$ is a prepoint. Define $p \models \mathcal{C}$ and $p \models (\mathcal{C} \Vdash \mathcal{D})$ by

$$\begin{array}{ll} p \models \mathcal{C} & \text{means } \forall X \in \mathcal{C}. p \models X \\ p \models (\mathcal{C} \Vdash \mathcal{D}) & \text{means } p \models \mathcal{C} \Rightarrow (\exists Y \in \mathcal{D}. p \models Y). \end{array}$$

Lemma 12.10 is a form of Modus Ponens, and a sanity check, and it will be useful:

LEMMA 12.10. Suppose $p \in \text{PrPt}$ is a prepoint and $\mathcal{C} \subseteq \text{Pred}$ and $X \in \text{Pred}$ is an internal predicate. Then if $p \models \mathcal{C}$ and $\mathcal{C} \Vdash X$ and $p \models (\mathcal{C} \Vdash X)$ then $p \models X$.

Proof. Direct from Definition 12.9. □

THEOREM 12.11 (Soundness). Suppose a prepoint $p \in \text{PrPt}$ generously names internal atoms (Definition 11.35). Suppose $\mathcal{C}, \mathcal{D} \subseteq \text{Pred}$ and suppose Γ and Δ are contexts. Then

- (1) $\Gamma \Vdash \Delta$ implies $p \models (\Gamma \Vdash \Delta)$, and
- (2) $\mathcal{C} \Vdash \mathcal{D}$ implies $p \models (\mathcal{C} \Vdash \mathcal{D})$.

Proof. It is not hard to check that part 2 follows from part 1. To prove part 1, we work by induction on derivations. We consider each rule in turn:

— We consider (Ax) . This follows from the fact that if $p \models X$ then $p \models X$.

— The rules (andL) , (andR) , (negL) , (negR) , and (Cut) are no harder.

— We consider (allL) . Choose $a' \in \mathbb{A}^{\text{level}(a)}$ and assume that

- if $p \models X'$ for every $X' \in \Gamma$ and $p \models X[a \mapsto a']$
- then $p \models Y$ for some $Y \in \Delta$.

Now suppose $p \models X'$ for every $X' \in \Gamma$ and suppose $p \models \forall a. X$. By Figure 3 (modall) $\forall a'' \in \mathbb{A}^{\text{level}(a)}. p \models (a'' a) \cdot X$. We assumed that p generously names internal atoms, so by Lemma 2.11(5) $p \models (a'' a) \cdot X$ for some $a'' \in \mathbb{A}^{\text{level}(a)}$ such that $p \models (a'' a) \cdot X \Leftrightarrow p \models X[a \mapsto a']$. Thus $p \models X[a \mapsto a']$.

It follows by our assumption above that $p \models Y$ for some $Y \in \Delta$.

— We consider (allR) . Assume for cosmall many a that

- if $p \models X'$ for every $X' \in \Gamma$,
- then $p \models (a' a) \cdot X$, or $p \models Y$ for some $Y \in \Delta$.

Now suppose $p \models X'$ for every $X' \in \Gamma$.

— If $p \models Y$ for some $Y \in \Delta$ then also $p \models \forall a. X$ or $p \models Y$ for some $Y \in \Delta$, and we are done; so

— suppose $p \not\models Y$ for every $Y \in \Delta$. It follows by inductive hypothesis that $p \models (a' a) \cdot X$ for cosmall many a' , and so by Figure 3 (**moda11**) that $p \models \forall a. X$. \square

COROLLARY 12.12. *Suppose $p \in \text{PrPt}$ generously names internal atoms, and suppose $C \subseteq \text{Pred}$. Then*

$$p \models C \quad \text{implies} \quad C \Vdash \perp.$$

In words: if a point that generously names internal atoms validates a set of predicates, then that set of predicates is consistent.

Proof. Suppose $C \Vdash \perp$. By Theorem 12.11 (since we assumed p generously names internal atoms) $p \models (C \Vdash \perp)$ and by Lemma 12.10 also $p \models \perp$, which by Lemma 5.9(3) is impossible. \square

Recall $\Theta \subseteq \text{Pred}$ from Definition 11.40. We have:

COROLLARY 12.13. $\Theta \Vdash \perp$. *Following Notation 12.5 we can write: Θ is consistent.*

Proof. Recall ext from Definition 11.19 and $\text{herb}(\text{ext}) \in \text{PrPt}$ from Definition 10.18. By Proposition 11.45(4) $\text{herb}(\text{ext}) \models \Theta$ and by Proposition 11.36 $\text{herb}(\text{ext})$ generously names internal atoms. We use Corollary 12.12. \square

12.1.3. Cut-admissibility

LEMMA 12.14. *Suppose Γ and Δ are contexts and σ is a substitution of atoms for atoms. Then if $\Gamma \Vdash \Delta$ is derivable then so is $\Gamma\sigma \Vdash \Delta\sigma$.*

Proof. By a standard induction on derivations. \square

REMARK 12.15. We only have Lemma 12.14 for substitutions of atoms for *atoms*—not substitutions of atoms for internal sets—because (**a11L**) has $X[a \mapsto a']$ on the upper left-hand side, not $X[a \mapsto u]$.²⁴

Likewise and for the same reasons, we only have Lemma 12.6 for a' , not for general u . This will not be a problem.

PROPOSITION 12.16 (Cut-admissibility). (**Cut**) from Figure 11 is admissible in the system without it.

Proof. By a standard proof, commuting instances of (**Cut**) upwards and eliminating essential cases. Eliminating the essential case between (**a11L**) and (**a11R**) uses Lemma 12.14. \square

12.2. Small substitutions

Notation 12.17 is standard but we give details anyway:

NOTATION 12.17. Suppose X and Y are sets and $f \in X \rightarrow Y$ is a partial function from X to Y . Write $\text{dom}(f) = \{x \in X \mid f(x) \text{ defined}\}$ for the **domain** of f and $\text{img}(f) = \{f(x) \mid x \in X, f(x) \text{ defined}\}$ for its **image**.

We build a sequence of *small substitutions* σ_γ in Definition 12.37:

DEFINITION 12.18. A **small substitution** is a partial function σ from atoms to internal sets such that:

- (1) $\text{dom}(\sigma)$ is small (so $\#\text{dom}(\sigma) \leq \aleph_\omega$).
- (2) If $a \in \text{dom}(\sigma)$ then $\sigma(a) \in \text{Set}^{\text{level}(a)}$.
- (3) $\text{dom}(\sigma) \# \text{img}(\sigma)$ (that is, for every $a \in \text{dom}(\sigma)$ and $x \in \text{img}(\sigma)$, $a \# x$).

REMARK 12.19. Condition 3 of Definition 12.18 is a convenience: it ‘avoids nameclash’ and so guarantees that sequential substitution coincides with the natural notion of simultaneous substitution, and helps simplify Definition 12.21. If in later work we consider a general theory of ‘small substitution’ for its own sake, then we might prefer to use just conditions 1 and 2.

²⁴The pedantic reader might note that we have not yet defined σ or $\Gamma\sigma$ and $\Delta\sigma$. However, these have their usual meanings, which are also special cases of the much more general material in Subsection 12.2, in particular Definition 12.21(2).

Lemma 12.20 is easy to prove with what we have so far, and will be useful:

LEMMA 12.20. *Suppose $\mathcal{D} \subseteq \text{Pred}$ is a small set of internal predicates and σ is a substitution and $\text{dom}(\sigma) \# \mathcal{D}$ (meaning by Notation 2.26 that $a \# \mathcal{D}$ for every $a \in \text{dom}(\sigma)$). Then $\mathcal{D}\sigma = \mathcal{D}$.*

Proof. By Lemma 2.51(4) $\text{dom}(\sigma) \# Y$ for every $Y \in \mathcal{D}$. The result follows using Lemma 4.9. \square

DEFINITION 12.21. If σ is a small substitution then:

- (1) Give σ an action $X\sigma$ on $X \in \text{Pred}$ by setting

$$X\sigma = X[a_1 \mapsto \sigma(a_1)] \dots [a_n \mapsto \sigma(a_n)] \quad \text{where} \quad \text{dom}(\sigma) \cap \text{supp}(X) = \{a_1, \dots, a_n\}.$$

Condition 3 of Definition 12.18 along with Corollary 4.14 ensure that the order of the a_1, \dots, a_n does not matter.

- (2) Give σ an action $\mathcal{C}\sigma$ on $\mathcal{C} \subseteq \text{Pred}$ by setting

$$\mathcal{C}\sigma = \{X\sigma \mid X \in \mathcal{C}\}.$$

- (3) Give σ an action $p \leftarrow \sigma$ on $p \in \text{PrPt}$ by setting

$$a \circ y \in p \leftarrow \sigma \Leftrightarrow p \models \text{elt}(y, a)\sigma.$$

DEFINITION 12.22. Suppose $\{\sigma_\alpha \mid \alpha < \lambda\}$ is a set of small substitutions such that

- (1) $\text{dom}(\sigma_\alpha) \# \text{dom}(\sigma'_{\alpha'})$ for every $\alpha, \alpha' < \lambda$ such that $\alpha \neq \alpha'$.
- (2) $\text{dom}(\sigma_\alpha) \# \text{img}(\sigma'_{\alpha'})$ for every $\alpha, \alpha' < \lambda$ (including $\alpha = \alpha'$).
- (3) $\bigcup_{\alpha < \lambda} \text{dom}(\sigma_\alpha)$ is small (that is, $\# \bigcup_{\alpha < \lambda} \text{dom}(\sigma_\alpha) \leq \aleph_\omega$).

Then write $\bigcup_{\alpha < \lambda} \sigma_\alpha$ for the small substitution mapping $a \in \text{dom}(\sigma_\alpha)$ to $\sigma_\alpha(a)$ and undefined otherwise.

If $\lambda = n$ is finite, then we might use standard \cup -infix notation and write $\sigma_0 \cup \dots \cup \sigma_{n-1}$.

LEMMA 12.23. *We continue the notation and conditions of Definition 12.22:*

- (1) $\bigcup_{\alpha < \lambda} \sigma_\alpha$ is a small substitution.
- (2) If $X \in \text{Pred}$ then

$$X\left(\bigcup_{\alpha < \lambda} \sigma_\alpha\right) = X\sigma_{\alpha_1} \dots \sigma_{\alpha_n},$$

for any finite subset $\{\alpha_1, \dots, \alpha_n\} \subset \lambda$ such that

$$\text{supp}(X) \cap (\text{dom}(\sigma_{\alpha_1}) \cup \dots \cup \text{dom}(\sigma_{\alpha_n})) = \text{supp}(X) \cap \bigcup_{\alpha < \lambda} \text{dom}(\sigma_\alpha),$$

and the order of the $\sigma_{\alpha_1}, \dots, \sigma_{\alpha_n}$ does not matter.

Proof. (1) $\bigcup_{\alpha < \lambda} \sigma_\alpha$ is a small substitution because we assumed in Definition 12.22 that $\bigcup_{\alpha < \lambda} \text{dom}(\sigma_\alpha)$ is small.

- (2) From clause 1 of Definition 12.21. \square

Lemma 12.24 extends Theorem 5.17:

LEMMA 12.24. *Suppose $p \in \text{PrPt}$ and $X \in \text{Pred}$ and σ is a small substitution. Then*

$$p \leftarrow \sigma \models X \Leftrightarrow p \models X\sigma.$$

Proof. By an induction on $\text{age}(X)$ mirroring the proof of Theorem 5.17. We use the assumption that σ is *small* in the case of all ; we give full details:

— *The case of $\text{and}(\mathcal{X})$ for $\mathcal{X} \subseteq_{fm} \text{Pred}$.* We reason as follows:

$$\begin{aligned} p \models \text{and}(\mathcal{X})\sigma &\Leftrightarrow p \models \text{and}(\{X\sigma \mid X \in \mathcal{X}\}) && \text{Figure 1}(\sigma\text{and}) \\ &\Leftrightarrow \forall X \in \mathcal{X}. p \models X\sigma && \text{Figure 3}(\text{modand}) \\ &\Leftrightarrow \forall X \in \mathcal{X}. p \leftarrow \sigma \models X && \text{IH } \text{age}(X) < \text{age}(\text{and}(\mathcal{X})) \end{aligned}$$

— *The case of $\text{neg}(X)$.* We reason as follows:

$$\begin{aligned} p \models \text{neg}(X)\sigma &\Leftrightarrow p \models \text{neg}(X\sigma) && \text{Figure 1}(\sigma\text{neg}) \\ &\Leftrightarrow p \not\models X\sigma && \text{Figure 3}(\text{modneg}) \\ &\Leftrightarrow p \leftarrow \sigma \not\models X && \text{IH } \text{age}(X) < \text{age}(\text{neg}(X)) \\ &\Leftrightarrow p \leftarrow \sigma \models \text{neg}(X) && \text{Figure 3}(\text{modneg}) \end{aligned}$$

— *The case of $\text{all}[b]X$ where $b \in \mathbb{A}^j$ for some $j \in \mathbb{Z}$.* Using Lemma 3.7(1) assume without loss of generality that b is fresh (so $b \# \sigma$; such a b exists since we assumed σ is small). Note by Theorem 2.31 and Corollary 2.28(1) (since $b', b \# \sigma, a$) that $(b' b) \cdot (p \leftarrow \sigma) = ((b' b) \cdot p) \leftarrow \sigma$. We reason as follows:

$$\begin{aligned} p \models (\text{all}[b]X)\sigma &\Leftrightarrow p \models \text{all}[b](X\sigma) && \text{Figure 1}(\sigma\text{all}) \text{ } b \# \sigma \\ &\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' b) \cdot p \models X\sigma && \text{Lemma 5.10} \\ &\Leftrightarrow \forall b' \in \mathbb{A}^j. (b' b) \cdot (p \leftarrow \sigma) \models X && \text{IH } \text{age}(X) < \text{age}(\text{all}[b]X) \\ &\Leftrightarrow p \leftarrow \sigma \models \text{all}[b]X && \text{Lemma 5.10} \end{aligned}$$

— *The case of $\text{elt}(y, b)$ for some $j \in \mathbb{Z}$ and $y \in \text{Set}^{j-1}$ and $b \in \text{Set}^j$.* We reason as follows:

$$p \models \text{elt}(y, b)\sigma \Leftrightarrow p \leftarrow \sigma \models \text{elt}(y, b) \quad \text{Clause 3 of Definition 12.21} \quad \square$$

One particular kind of small substitution will be of particular interest; a small substitution (in fact, it has countably infinite domain) that is intuitively the ϑ -ambiguous closure of $[a \mapsto x]$ (ϑ is the shift permutation fixed in Definition 11.2):

DEFINITION 12.25. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and suppose $\vartheta^j(a) \# \vartheta^k \cdot x$ for every $j, k \in \mathbb{Z}$ —or equivalently, $\vartheta^{\mathbb{Z}} \cdot a \# \vartheta^{\mathbb{Z}} \cdot x$. Then define $[a \mapsto x]$ by

- $[a \mapsto x](\vartheta^j(a)) = \vartheta^j \cdot x$ for $j \in \mathbb{Z}$.
- $[a \mapsto x](b)$ is undefined for all other atoms b .

If $p \in \text{PrPt}$ then we might write

$$p \leftarrow [a \mapsto x] \quad \text{as} \quad p[x \leftarrow a].$$

LEMMA 12.26. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and $\vartheta^{\mathbb{Z}} \cdot a \# \vartheta^{\mathbb{Z}} \cdot x$. Then:

- (1) $[a \mapsto x]$ is a small substitution (Definition 12.18).
- (2) $[a \mapsto x]$ is ϑ -ambiguous, meaning that $\vartheta \cdot [a \mapsto x] = [a \mapsto x]$.

Proof. We note that $\text{dom}([a \mapsto x])$ is countably infinite and so small. It is ϑ -ambiguous by construction in Definition 12.25. \square

Recall **ATOMI** from Figure 10:

LEMMA 12.27. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$ and $\vartheta^{\mathbb{Z}} \cdot a \# \vartheta^{\mathbb{Z}} \cdot x$ so that by Definition 12.25 $[a \mapsto x]$ is defined. Then

$$p \models \text{ATOMI} \quad \text{implies} \quad p[x \leftarrow a] \models \text{ATOMI}.$$

Proof. Consider $X \in \text{Pred}$ and $i' \in \mathbb{Z}$ and $a' \in \mathbb{A}^{i'}$ and $u' \in \text{Set}^{i'}$ and $b' \in \mathbb{A}^{i'-1}$. By Lemma 5.9 it suffices to show that $p[x \leftarrow a] \models X$ if and only if $p[x \leftarrow a] \models X[a' \mapsto [b'] (b' \in u')]$. Using Lemma 4.7 we may assume without loss of generality that $b' \# [a \leftarrow x]$, that is, $b' \# \vartheta^{\mathbb{Z}} \cdot a, \vartheta^{\mathbb{Z}} \cdot x$.

Choose $a'' \in \mathbb{A}^i$ fresh (so $a'' \# X$, $\vartheta^{\mathbb{Z}} \cdot a$, $\vartheta^{\mathbb{Z}} \cdot x$ and $a'' \# [a \mapsto x]$). We reason as follows:

$$\begin{aligned}
p[x \mapsto a] &\models X[a' \mapsto [b'] (b' \in u')] \\
&\Leftrightarrow p \models X[a' \mapsto [b'] (b' \in u')] [a \mapsto x] && \text{Lemma 12.24} \\
&\Leftrightarrow p \models ((a'' a') \cdot X)[a' \mapsto [b'] (b' \in u')] [a \mapsto x] && \text{Lemma 4.7 } a'' \# X \\
&\Leftrightarrow p \models ((a'' a') \cdot X)[a \mapsto x] [a'' \mapsto ([b'] (b' \in u'))] [a \mapsto x] && \text{Using Lemma 4.12 } a'' \# [a \mapsto x] \\
&\Leftrightarrow p \models ((a'' a') \cdot X)[a \mapsto x] [a'' \mapsto [b'] (b' \in u' [a \mapsto x])] && \text{Figure 1 } (\sigma[]) \ b' \# [a \mapsto x] \\
&\Leftrightarrow p \models ((a'' a') \cdot X)[a \mapsto x] [a'' \mapsto u' [a \mapsto x]] && p \models \text{ATOMI} \\
&\Leftrightarrow p \models ((a'' a') \cdot X)[a' \mapsto u'] [a \mapsto x] && \text{Using Lemma 4.12 } a'' \# [a \mapsto x] \\
&\Leftrightarrow p \models X[a' \mapsto u'] [a \mapsto x] && \text{Lemma 4.7 } a'' \# X \\
&\Leftrightarrow p[x \mapsto a] \models X[a' \mapsto u'] && \text{Lemma 12.24} \quad \square
\end{aligned}$$

PROPOSITION 12.28. Suppose $p \in \text{PrPt}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$. Then

$$p \models \Theta \quad \text{implies} \quad p[x \mapsto a] \models \Theta.$$

Proof. Suppose $p \models \Theta$. Unpacking Definition 11.40, $p \models \Theta$ means $p \models \vartheta\text{-AMBIG}$ and $p \models \text{EXTEN}$ and $p \models \text{ATOMI}$.

- Suppose $p \models \vartheta\text{-AMBIG}$, so that by Lemma 11.42 $\vartheta \cdot p = p$. By Theorem 2.31 and Lemma 12.26(2) we have $\vartheta \cdot (p[x \mapsto a]) = p$, and by Lemma 11.42 $p[x \mapsto a] \models \vartheta\text{-AMBIG}$.
- By Lemmas 12.24 and 12.20 (since every predicate in EXTEN is closed) $p[x \mapsto a] \models \text{EXTEN}$.
- By Lemma 12.27 $p[x \mapsto a] \models \text{ATOMI}$.

It follows that $p[x \mapsto a] \models \Theta$. \square

12.3. We build a maximally consistent set $\text{maxfilt}(\Theta)$

12.3.1. *Some preliminaries.* Definition 12.29 mirrors Definition 10.10, but for sets of internal predicates instead of equality theories:

DEFINITION 12.29. Suppose $\mathcal{C} \subseteq \text{Pred}$ is a set of internal predicates. Define $[\mathcal{C}]_{\text{pd}}$ the **deductive closure** of \mathcal{C} by

$$[\mathcal{C}]_{\text{pd}} = \{X \in \text{Pred} \mid \mathcal{C} \vdash_{\text{pd}} X\}.$$

It is clear from Definition 12.29 that $X \in [\mathcal{C}]_{\text{pd}}$ if and only if $\mathcal{C} \vdash_{\text{pd}} X$ and that $[\mathcal{C}]_{\text{pd}}$ is the least deductively closed set containing \mathcal{C} .

LEMMA 12.30. If Δ is a context then $\mathcal{C} \vdash_{\text{pd}} \Delta$ if and only if $[\mathcal{C}]_{\text{pd}} \vdash_{\text{pd}} \Delta$.

Proof. The left-to-right implication is immediate from Definition 12.29. The right-to-left implication follows by standard reasoning using Proposition 12.16. \square

A technical definition will help in Definition 12.37:

DEFINITION 12.31. Suppose $A \subseteq \mathbb{A}$ is a small set of atoms and $i \in \mathbb{Z}$ and $x', x \in \text{Set}^i$. Choose fresh $c \in \mathbb{A}^i$ (so $c \# \vartheta^{\mathbb{Z}} \cdot A$, $\vartheta^{\mathbb{Z}} \cdot x'$, $\vartheta^{\mathbb{Z}} \cdot x$). Then define $\text{IFF}_A(x, x')$ by

$$\text{IFF}_A(x, x') = \{X[c \mapsto x] \Leftrightarrow X[c \mapsto x'] \mid X \in \text{Pred}, \text{supp}(X) \subseteq A \cup \vartheta^{\mathbb{Z}} \cdot c\}.$$

($\vartheta^{\mathbb{Z}} \cdot c$ is from Notation 11.1.)

REMARK 12.32. Intuitively $\text{IFF}_A(x', x)$ is a set of internal predicates asserting $\vartheta^i \cdot x'$ and $\vartheta^i \cdot x$ are Leibniz equal for any $i \in \mathbb{Z}$, where ‘Leibniz equal’ = “cannot be distinguished by any permitted observation”. The permitted observations are predicates X with support limited to $A \subseteq \mathbb{A}$ and some choice of atom c to substitute for x' and x .

We will use this in clauses 2 and 3 of Definition 12.37.

LEMMA 12.33. Suppose $p \in \text{PrPt}$ and $A \subseteq \mathbb{A}$ is small and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $x \in \text{Set}^i$, and suppose $\vartheta^{\mathbb{Z}} \cdot a \# A$ (so that, since A is small, also $a \notin A$) and $\vartheta^{\mathbb{Z}} \cdot a \# x$. Then:

- (1) $\text{IFF}_A(a, x)[a \xrightarrow{\vartheta} x] = \text{IFF}_A(x, x)$.
- (2) $p \models \text{IFF}_A(x, x)$.
- (3) As a corollary, $p[x \xleftarrow{\vartheta} a] \models \text{IFF}_A(a, x)$.

Proof. (1) Unpacking Definitions 12.31 and 12.21(2) we see that, in the notation of Definition 12.31, it suffices to show that for $a \# X$,

$$X[c \mapsto a][a \mapsto x] = X[c \mapsto x] \quad \text{and} \quad X[c \mapsto x][a \mapsto x] = X[c \mapsto x].$$

The left-hand equality follows from Corollary 4.15 and Figure 1 ($\sigma\alpha$). The right-hand equality can be deduced using Corollary 4.14 and Lemma 4.9.

- (2) By easy reasoning from Definition 12.31 and 5.9(2).
- (3) We combine parts 1 and 2 of this result with Lemma 12.24. □

12.3.2. We build the set

REMARK 12.34. We can compare Definitions 11.3 and 11.8 and Remark 11.10, with Definition 12.35(2&3) and Remark 12.36 below.

All concern ‘triangular’ enumerations, but there is a significant difference: the enumerations of Definitions 11.3 and 11.8 do not include repeats, whereas the enumeration of Definition 12.35(2&3) does include repeats, and plenty of them.

The enumerations are similar in the sense that in both cases, we aim to guarantee ‘generous’ supplies of atoms naming internal sets. The relevant result in the case of Definition 12.35 is Lemma 12.45; for Definitions 11.6 and 11.8 see generosity of \mathcal{A}_β in Proposition 11.30.

- DEFINITION 12.35(1) Enumerate $\mathbb{A}^1 \times \text{Pred}$ as $(a_{\beta'}, X_{\beta'})$ where $\beta' < \varpi$ (ϖ is from Notation 11.9).
- (2) Define another ‘triangular’ enumeration, which includes repeats, $(a_{\alpha\beta}, X_{\alpha\beta})$ where $\beta \leq \alpha < \varpi$ and for every $\alpha < \varpi$ and $\beta \leq \alpha$ we have $(a_{\alpha\beta}, X_{\alpha\beta}) = (a_\beta, X_\beta)$.
Thus if $\beta = \beta'$ and $\beta \leq \alpha$ and $\beta' \leq \alpha'$ and α is *not* necessarily equal to α' , then $(a_{\alpha\beta}, X_{\alpha\beta}) = (a_{\alpha'\beta'}, X_{\alpha'\beta'})$.
 - (3) Write (a_γ, X_γ) for the γ th element in the triangular enumeration, and write

$$x_\gamma = [a_\gamma]X_\gamma.$$

REMARK 12.36. An initial segment of the triangular enumeration in Definition 12.35 is as follows:

- For $\gamma=0$ and $\alpha = \beta = 0$ we have (a_0, X_0) .
- For $\gamma=1$ and $\alpha = 1$ and $\beta = 0$ we have (a_1, X_1) and $(a_1, X_1) = (a_0, X_0)$.
- For $\gamma=2$ and $\alpha = 1$ and $\beta = 1$ we have (a_2, X_2) .
- For $\gamma=3$ and $\alpha = 2$ and $\beta = 0$ we have (a_3, X_3) and $(a_3, X_3) = (a_1, X_1) = (a_0, X_0)$.
- For $\gamma=4$ and $\alpha = 2$ and $\beta = 1$ we have (a_4, X_4) and $(a_4, X_4) = (a_2, X_2)$.
- For $\gamma=5$ and $\alpha = 2$ and $\beta = 2$ we have (a_5, X_5) .
- For $\gamma=6$ and $\alpha = 3$ and $\beta = 0$ we have (a_6, X_6) and $(a_6, X_6) = (a_3, X_3) = (a_1, X_1) = (a_0, X_0)$.
- ... and so on.

We are now ready to build our maximally consistent set, using $\text{herb}(\text{ext})$:

DEFINITION 12.37. We define a sequence of triples $(A_\gamma, \sigma_\gamma, \mathcal{C}_\gamma)$ where $\gamma < \varpi$ and $A_\gamma \subseteq \mathbb{A}$ is a set of atoms and σ_γ is a small substitution and $\mathcal{C}_\gamma \subseteq \text{Pred}$ as follows, where for brevity we write

$$p_\gamma \quad \text{for} \quad \text{herb}(\text{ext}) \leftarrow \sigma_\gamma :$$

(1) We define:

$$\begin{aligned} A_0 &= \emptyset \\ \sigma_0 &= \emptyset \\ \mathcal{C}_0 &= \emptyset \end{aligned}$$

(So σ_0 is the unique smallest small substitution, with empty domain, and $p_0 = \text{herb}(\text{ext})$.)

(2) Suppose σ_γ and \mathcal{C}_γ are defined and $p_\gamma \models \Theta, \mathcal{C}_\gamma, \forall a_\gamma. X_\gamma$.
Define

$$A_{\gamma+1} = A_\gamma \cup \text{supp}(\mathcal{C}_\gamma) \cup \vartheta^\mathbb{Z}.a \cup \vartheta^\mathbb{Z}.\text{supp}(X_\gamma).$$

Let a''_γ be some choice²⁵ of atom fresh for $A_{\gamma+1}$ and define (recall \cup for small substitutions from Definition 12.22):

$$\begin{aligned} \sigma_{\gamma+1} &= \sigma_\gamma \cup [a''_\gamma \mapsto x_\gamma] \\ \mathcal{C}_{\gamma+1} &= \mathcal{C}_\gamma, \forall a_\gamma. X_\gamma, \text{IFF}_{A_{\gamma+1}}(a''_\gamma, x_\gamma) \end{aligned}$$

(Recall from Definition 12.35 that $x_\gamma = [a_\gamma]X_\gamma$.)

(3) Suppose σ_γ and \mathcal{C}_γ are defined and $p_\gamma \models \Theta, \mathcal{C}_\gamma, \neg \forall a_\gamma. X_\gamma$.

From Figure 3 (**modall**) there exist generously many, and so at least one, $a' \in \mathbb{A}^{\text{level}(a_\gamma)}$ such that $p_\gamma \models \neg X[a_\gamma \mapsto a']$.

Define

$$A_{\gamma+1} = A_\gamma \cup \text{supp}(\mathcal{C}_\gamma) \cup \vartheta^\mathbb{Z}.a_\gamma \cup \vartheta^\mathbb{Z}.\text{supp}(X_\gamma) \cup \vartheta^\mathbb{Z}.a'.$$

Let $a''_\gamma \in \mathbb{A}^0$ be some choice of atom fresh for $A_{\gamma+1}$ and define:

$$\begin{aligned} \sigma_{\gamma+1} &= \sigma_\gamma \cup [a''_\gamma \mapsto x_\gamma] \\ \mathcal{C}_{\gamma+1} &= \mathcal{C}_\gamma, \neg \forall a_\gamma. X_\gamma, \neg X[a_\gamma \mapsto a'], \text{IFF}_{A_{\gamma+1}}(a''_\gamma, x_\gamma) \end{aligned}$$

(4) If $\lambda \leq \varpi$ is a limit ordinal strictly less than ϖ then define:

$$\begin{aligned} A_\lambda &= \bigcup_{\gamma < \lambda} A_\gamma \\ \sigma_\lambda &= \bigcup_{\gamma < \lambda} \sigma_\gamma \\ \mathcal{C}_\lambda &= \bigcup_{\gamma < \lambda} \mathcal{C}_\gamma \end{aligned}$$

(5) Finally, we define

$$\text{maxfilt}(\Theta) = [\Theta \cup \bigcup_{\gamma < \varpi} \mathcal{C}_\gamma]_{\text{pd}}.$$

REMARK 12.38. We take a deductive closure when we define $\text{maxfilt}(\Theta)$ for the technical reason that the algorithm in Definition 12.37 only puts internal predicates into \mathcal{C}_γ that have the form $\forall a. X$ (or $X \Leftrightarrow Y$). Thus, some predicates are ‘missing’; for instance $\text{and}(\emptyset)$, otherwise known as **T**, though $\forall a. \text{T}$ will be present.

In fact, for every X there exists an $a \# X$ such that one of $\forall a. X$ or $\neg \forall a. X$ is placed in \mathcal{C}_γ , and these are derivably equivalent to X and $\neg X$ respectively, so the missing predicates are present up to derivable equivalence. Taking deductive closure adjusts for this.

REMARK 12.39. A step back to look briefly at the big picture: we want to construct a point. This point is ‘trying’ to be $\text{herb}(\text{ext}) \leftarrow \sigma_\varpi$, but that is not well-defined because σ_ϖ is not a small substitution.²⁶

In fact we can still get the effect of $\text{herb}(\text{ext}) \leftarrow \sigma_\varpi$; we just have to go about it more subtly, using maximally consistent sets of predicates. This is the reason for $\text{maxfilt}(\Theta)$, out of which we will eventually derive the point we want. This is $G(\text{maxfilt}(\Theta))$; see Definition 12.48 onwards.

Before we get to that definition we have work to do; but everything is now in place.

²⁵This choice can be made canonically as “the least available atom”, if atoms are delivered to us with some well-ordering.

²⁶If we try to generalise to large substitutions and then define and manipulate σ_ϖ , then the point of failure—where the proofs fail—is Lemma 12.24. This requires its substitution σ to be small, for the case of **all**.

12.3.3. *Consistency of the set.* A technical lemma will be useful:

LEMMA 12.40. *Suppose $\lambda < \varpi$ is a limit ordinal and suppose $\gamma < \lambda$. Then*

$$\sigma_\lambda = \sigma_\gamma \cup \bigcup_{\gamma < \alpha < \lambda} [a''_\alpha \mapsto x_\alpha] \quad \text{and} \quad p_\lambda = p_\gamma \leftarrow \left(\bigcup_{\gamma < \alpha < \lambda} [a''_\alpha \mapsto x_\alpha] \right).$$

Proof. The left-hand equality is by construction in Definition 12.37. The right-hand equality can be deduced using the left-hand equality and Lemmas 12.24 and 5.11. \square

PROPOSITION 12.41(1) *$\text{herb}(\text{ext}) \leftarrow \sigma_\gamma \models \Theta, \mathcal{C}_\gamma$ for every $\gamma < \varpi$.*

(2) *$\Theta, \mathcal{C}_\gamma \not\models \perp$ for every $\gamma < \varpi$, and $\text{maxfilt}(\Theta) \not\models \perp$.*

Proof. Part 2 follows from part 1 using Corollary 12.12 (for $\gamma < \varpi$) and Lemma 12.8 (for $\text{maxfilt}(\Theta)$).

We prove part 1 by induction on $\gamma \leq \varpi$. For brevity write $p_\gamma = \text{herb}(\text{ext}) \leftarrow \sigma_\gamma$ for $\gamma < \varpi$. We consider the possibilities in turn:

- (1) By Proposition 11.45(4) $\text{herb}(\text{ext}) \models \Theta$.
- (2) Suppose $p_\gamma \models \Theta, \mathcal{C}_\gamma$ and suppose clause 2 is activated in Definition 12.37 because $p_\gamma \models \forall a_\gamma. X_\gamma$. $\mathcal{C}_{\gamma+1}$ consists of the following components:
 - a small set \mathcal{C}_γ for which $\vartheta^\mathbb{Z}.a''_\gamma$ is fresh,
 - $\forall a_\gamma. X_\gamma$ for which using Lemma 2.63 $\vartheta^\mathbb{Z}.a''_\gamma$ is fresh, and
 - $\text{IFF}_{A_{\gamma+1}}(a''_\gamma, x_\gamma)$.

It follows from Lemma 12.40 (or just direct from the construction) that $p_{\gamma+1} = p_\gamma[x_\gamma \leftarrow a]$, so we can note that:

- By Proposition 12.28 $p_{\gamma+1} \models \Theta$, because $p_\gamma \models \Theta$.
- By Lemmas 12.24 and 12.20 $p_{\gamma+1} \models \mathcal{C}_\gamma$ and $p_{\gamma+1} \models \forall a_\gamma. X_\gamma$ and so $p_{\gamma+1} \models X_\gamma$ because $\vartheta^\mathbb{Z}.a''_\gamma \# \mathcal{C}_\gamma$ and $\vartheta^\mathbb{Z}.a''_\gamma \# \forall a_\gamma. X_\gamma$.
- By Lemma 12.33(3) $p_{\gamma+1} \models \text{IFF}_{A_{\gamma+1}}(a, x_\gamma)$.

Thus $p_{\gamma+1} \models \Theta, \mathcal{C}_{\gamma+1}$.

- (3) The case that $p_\gamma \models \Theta, \mathcal{C}_\gamma$ and clause 3 is activated in Definition 12.37 because $p_\gamma \not\models \forall a_\gamma. X_\gamma$ is very similar to the previous clause.
- (4) Suppose $\lambda \leq \varpi$ is a limit ordinal strictly less than ϖ . Suppose $X \in \Theta \cup \mathcal{C}_\lambda$. Then $X \in \Theta \cup \mathcal{C}_\gamma$ for some $\gamma < \lambda$. Using Lemmas 12.40, 12.24, and 4.9 we have

$$p_\lambda \models X \stackrel{\text{L12.40}}{\Leftrightarrow} p_{\gamma+1} \leftarrow \bigcup_{\gamma < \alpha < \lambda} [a''_\alpha \mapsto x_\alpha] \models X \stackrel{\text{L12.24}}{\Leftrightarrow} p_{\gamma+1} \models X \left(\bigcup_{\gamma < \alpha < \lambda} [a''_\alpha \mapsto x_\alpha] \right) \stackrel{\text{L4.9}}{\Leftrightarrow} p_{\gamma+1} \models X.$$

We use the inductive hypothesis. \square

LEMMA 12.42. *$\text{maxfilt}(\Theta)$ from Definition 12.37 is consistent.*

Proof. From Proposition 12.41(2) and Lemma 12.30. \square

12.3.4. Other properties of $\text{maxfilt}(\Theta)$

LEMMA 12.43(1) *$\text{maxfilt}(\Theta)$ from Definition 12.37 is deductively closed.*

- (2) *For every $X \in \text{Pred}$, precisely one of $X \in \text{maxfilt}(\Theta)$ or $\neg X \in \text{maxfilt}(\Theta)$ holds.*
- (3) *$\text{maxfilt}(\Theta)$ is maximally consistent.*

Proof. (1) $\text{maxfilt}(\Theta)$ is deductively closed by the use of deductive closure $[-]_{\text{bd}}$ in clause 5 of Definition 12.37.

- (2) By the structure of the algorithm in Definition 12.37, for every $a \in \mathbb{A}$ at least one of $\forall a.X$ or $\neg \forall a.X$ must be in $\text{maxfilt}(\Theta)$.

We may choose $a \# X$, and so by Lemma 12.7 and deductive closure (part 1 of this result) at least one of X or $\neg X$ must be in $\text{maxfilt}(\Theta)$. We cannot have both, since this would contradict Lemma 12.42.

- (3) Maximality follows from Lemma 12.42 by standard arguments of propositional logic. \square

LEMMA 12.44. $\text{maxfilt}(\Theta)$ is ϑ -ambiguous. That is:

$$\vartheta \cdot \text{maxfilt}(\Theta) = \text{maxfilt}(\Theta).$$

Proof. Consider some $X \in \text{maxfilt}(\Theta)$. By construction $\Theta \subseteq \text{maxfilt}(\Theta)$ so in particular $X \Leftrightarrow \vartheta \cdot X \in \text{maxfilt}(\Theta)$. By deductive closure (Lemma 12.43(1)) it follows that $\vartheta \cdot X \in \text{maxfilt}(\Theta)$. The reverse implication is no harder. \square

LEMMA 12.45. Suppose $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $u \in \text{Set}^i$. Then

$$\exists a'' \in \mathbb{A}^i. ((a'' \cdot a) \cdot X \in \text{maxfilt}(\Theta) \Leftrightarrow X[a \mapsto u] \in \text{maxfilt}(\Theta)).$$

Abusing Definition 8.1 (which is for points, not sets of predicates) we could say that $\text{maxfilt}(\Theta)$ generously names internal sets; we make this formal in Corollary 12.51.

Proof. Consider some $X \in \text{Pred}$ and $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $u \in \text{Set}^i$. There are now two sub-cases:

- (1) Suppose u is an internal comprehension (Notation 3.2).

Then let γ be some stage in the triangular enumeration of Definition 12.35 such that $[a_\gamma]X_\gamma = u$ and $\text{supp}(X) \subseteq A_{\gamma+1}$.

It is a fact of the construction that there are generously many such γ , and clauses 2 and 3 of Definition 12.37 associate to each of them a fresh atom a''_γ and add $X[a \mapsto a''_\gamma] \Leftrightarrow X[a \mapsto u] \in \text{IFF}_{A_{\gamma+1}}(a''_\gamma, u)$ to $\mathcal{C}_{\gamma+1}$. By Lemma 4.17 $X[a \mapsto a''_\gamma] = (a''_\gamma \cdot a) \cdot X$.

- (2) Suppose $u = \text{atm}(n)$ for $n \in \mathbb{A}^i$ is an internal atom (which may or may not be equal to a).

By construction $\text{ATOMI} \subseteq \Theta \subseteq \text{maxfilt}(\Theta)$ and by Lemma 4.16 $X = X[n \mapsto \text{atm}(n)]$. Using deductive closure (Lemma 12.43(1)) $X \in \text{maxfilt}(\Theta)$ if and only if $X[n \mapsto [b](b \in n)] \in \text{maxfilt}(\Theta)$, for any $X \in \text{Pred}$ and $b \in \mathbb{A}^{i-1}$ other than n . Now $[b](b \in n)$ is an internal comprehension, so this case is reduced to the previous case. \square

LEMMA 12.46. Suppose $X, Y \in \text{Pred}$. Then:

- (1) $\text{and}(\mathcal{X}) \in \text{maxfilt}(\Theta)$ if and only if $\forall X \in \mathcal{X}. X \in \text{maxfilt}(\Theta)$.
 (2) $\text{neg}(X) \in \text{maxfilt}(\Theta)$ if and only if $X \notin \text{maxfilt}(\Theta)$.

Proof. If $\text{and}(\mathcal{X})$ then by deductive closure (Lemma 12.43(1)) and Figure 11 $X \in \text{maxfilt}(\Theta)$ for every $X \in \mathcal{X}$. The reverse implication is similar.

The case of neg is immediate from Lemma 12.43(2). \square

LEMMA 12.47. Suppose $i \in \mathbb{Z}$ and $a \in \mathbb{A}^i$ and $X \in \text{Pred}$. Then the following conditions are equivalent:

$$\begin{aligned} & \forall a'. X \in \text{maxfilt}(\Theta) \\ \Leftrightarrow & \forall a' \in \mathbb{A}^i. X[a \mapsto a'] \in \text{maxfilt}(\Theta) \\ \Leftrightarrow & \forall u \in \text{Set}^i. X[a \mapsto u] \in \text{maxfilt}(\Theta) \\ \Leftrightarrow & \forall a' \in \mathbb{A}^i. (a' \cdot a) \cdot X \in \text{maxfilt}(\Theta) \end{aligned}$$

Proof. By Lemma 12.43(1) $\text{maxfilt}(\Theta)$ is deductively closed. Suppose $\forall a'. X \in \text{maxfilt}(\Theta)$.

— Note from Notation 3.2 that if $a' \in \mathbb{A}^i$ then $\text{atm}(a') \in \text{Set}^i$ ($X[a \mapsto a']$ is shorthand for $X[a \mapsto \text{atm}(a')]$).

By Lemma 12.6 and deductive closure (Lemma 12.43(1)) $\forall a' \in \mathbb{A}^i. X[a \mapsto a'] \in \text{maxfilt}(\Theta)$.

- Note by Lemma 4.17 that $X[a \mapsto a'] = (a' \# a) \cdot X$ if $a' \# X$. Then using Lemma 12.45 we deduce $\forall u \in \text{Set}^i. X[a \mapsto u] \in \text{maxfilt}(\Theta)$.
- It also follows that $\forall a' \in \mathbb{A}^i. (a' \# a) \cdot X \in \text{maxfilt}(\Theta)$.

Now suppose $\forall a' \in \mathbb{A}^i. (a' \# a) \cdot X \in \text{maxfilt}(\Theta)$. There are two cases:

- Suppose $\forall a. X \in \text{maxfilt}(\Theta)$ is introduced by clause 2 of Definition 12.37. Then we are done.
- Suppose $\neg \forall a. X \in \text{maxfilt}(\Theta)$ is introduced by clause 3 of Definition 12.37. Then also $\neg X[a \mapsto a']$ is introduced for some atom $a' \in \mathbb{A}^i$. By Lemma 12.45 (taking $u = \text{atm}(a')$ in that Lemma) it follows that $\exists a'' \in \mathbb{A}^i. (a'' \# a) \cdot \neg X \in \text{maxfilt}(\Theta)$, so that by Lemma 12.46(2) $\exists a'' \in \mathbb{A}^i. (a'' \# a) \cdot X \notin \text{maxfilt}(\Theta)$. From Lemma 2.11(5) we contradict our assumption that $\forall a'' \in \mathbb{A}^i. (a'' \# a) \cdot X \in \text{maxfilt}(\Theta)$. Thus this case is impossible. \square

12.3.5. We build a point

DEFINITION 12.48. Define maps F mapping $p \in \text{PrPt}$ to $F(p) \subseteq \text{Pred}$ and G mapping $\mathcal{C} \subseteq \text{Pred}$ to $G(\mathcal{C}) \in \text{PrPt}$ as follows:

$$\begin{aligned} F : p &\mapsto \{X \mid p \models X\} \\ G : \mathcal{C} &\mapsto \{a \circ x \mid x \in a \in \mathcal{C}\} \end{aligned}$$

PROPOSITION 12.49(1) $G(\text{maxfilt}(\Theta)) \models X$ if and only if $X \in G(\text{maxfilt}(\Theta))$.
 (2) $FG(\text{maxfilt}(\Theta)) = \text{maxfilt}(\Theta)$.

Proof. Part 2 just rephrases part 1 using Definition 12.48.

With what we have so far, part 1 is by a routine induction on X :

- *The case of $\text{elt}(x, a)$.* From Figure 3 (**modelt**) and Definition 12.48.
- *The case of $\text{and}(\mathcal{X})$.* From Figure 3 (**modand**) and Lemma 12.46(1).
- *The case of $\text{neg}(X')$.* From Figure 3 (**modneg**) and Lemma 12.46(2).
- *The case of $\text{all}[a]X'$.* From Figure 3 (**modall**) and Lemma 12.47. \square

LEMMA 12.50. $G(\text{maxfilt}(\Theta))$ is extensional (Definition 8.3(2)).

Proof. By construction in Definition 11.40 $\text{EXTEN} \subseteq \Theta$ and so in particular

$$\forall a. \forall a'. (\forall b. (b \in a \Leftrightarrow b \in a')) \Rightarrow (\forall c. (a \in c \Leftrightarrow a' \in c)) \in \Theta$$

where a, a', b , and c are atoms of appropriate levels. By construction in Definition 12.37(5) $\Theta \subseteq \text{maxfilt}(\Theta)$ and therefore by Proposition 12.49

$$G(\text{maxfilt}(\Theta)) \models \forall a. \forall a'. (\forall b. (b \in a \Leftrightarrow b \in a')) \Rightarrow (\forall c. (a \in c \Leftrightarrow a' \in c)).$$

It follows using Proposition 12.49 and Lemma 12.47 (and Lemma 6.6) that

$$G(\text{maxfilt}(\Theta)) \models u = u' \quad \text{implies} \quad \forall z. (p \models u \in z \Leftrightarrow p \models u' \in z).$$

It follows by Corollary 7.7 that

$$G(\text{maxfilt}(\Theta)) \models u = u' \quad \text{implies} \quad G(\text{maxfilt}(\Theta)) \models u = u'$$

as required. \square

COROLLARY 12.51. $G(\text{maxfilt}(\Theta))$ is a point (Definition 8.3).

Proof. We consult Definition 8.3 and see we it suffices to check that $G(\text{maxfilt}(\Theta))$ generously names internal sets, and is extensional and ϑ -ambiguous.

- $G(\text{maxfilt}(\Theta))$ generously names internal sets by Lemma 12.45 and Proposition 12.49(1).
- $G(\text{maxfilt}(\Theta))$ is extensional by Lemma 12.50.
- $G(\text{maxfilt}(\Theta))$ is ϑ -ambiguous by Lemma 12.44 and Theorem 2.31.

The result follows. □

We can now prove:

THEOREM 12.52. *NF [Qui37] is consistent.*

Proof. NF is known consistent relative to TST+ [Spe62]. By Corollary 9.30 TST+ is consistent if points exist. By Corollary 12.51 points exist. □

REMARK 12.53. We conclude with some comments on the treatment of \forall . Universal quantification is probably the most ‘explosive’ component of our syntax because it is impredicative: universal quantification quantifies over all x (which, for instance, is highly likely to destroy inductive quantities).

We employ various strategies to sidestep this danger:

- Initially we model \forall using \mathcal{U} in Figure 3 (moda11). This preserves induction and gives us some simple proofs, however, it is not sound in general for “ $\forall a. \phi \Rightarrow \phi[a \mapsto x]$ ”.
- In the entailment relation of Figure 11 \forall is modelled by ‘for all atoms’. This gives “ $\forall a. \phi \Rightarrow \phi[a \mapsto b]$ ”; still not sound for all x , but stronger than the model using \mathcal{U} . By this point we have *herb*(ext), which generously names its internal atoms and so can soundly interpret this stronger rule.
- In TST+ \forall is modelled (as it must be) by ‘for all elements / for all terms’. Only in Definition 12.37 do we model this directly, using a hybrid approach as discussed at the start of this Section.

13. CONCLUSIONS

The consistency of NF itself solves a longstanding open problem and reassures us that we can indeed reason in set theory with a universal set. The mathematics seems fairly general, and we hope it might be applied to solve more problems.

Given our proof, we can examine it to see how much set-theoretic strength it really uses, and thus see relative to what system we have proved NF consistent.²⁷ We have not used the Axioms of Choice or Replacement in the proofs of this paper: we have proved NF consistent relative to Zermelo set theory (**Z**).

The proofs of this paper are not short, but they are fairly systematic. Much of the design has been guided by what we saw in [Gab16; GG16], especially the aspects to do with duality and amgis; if these one day become common mathematical knowledge then this material may seem much simpler.

For instance, we did not have to give the reader examples and detailed definitions for sets, functions and function application, powersets, cardinality, or universal quantification—the principles of Equivariance and Conservation of Support, atoms-abstraction, support, freshness, the \mathcal{U} -quantifier, and the sigma- and amgis-actions may one day similarly be taken for granted.

As is often the case, much of the difficulty has been in getting the right definitions.

13.1. Future work

Consider that the structure of points $a \circ x$ resembles that of a λ -term in normal form, if we read $a \circ x$ as ‘ a applied to x ’. It is natural to generalise this to $a \circ x_1 \circ \dots \circ x_n$ and try to build stratified models of the λ -calculus, following the philosophy of “ λ as a universal quantifier” from e.g. [GG10; GG16], in which λ -terms are interpreted as sets of points and λ -abstraction as a variant of \forall -quantification. One motivation for doing this is that it might lead to new *dependent type theories*, since the models, being

²⁷Consistency proofs are always *relative* to another foundation. So for instance: ZFA set theory is consistent *relative to* ZF set theory—meaning that if ZF is consistent then so is ZFA; and the FM set theory underlying nominal techniques was originally developed to prove ZFA+ \neg AC consistent relative to ZFA [Fra22].

So, the sentence “NF is consistent” must necessarily continue with “relative to system X”, for some value of X. Any value of X would do, but generally speaking the more weak X is the more interesting the result. For more on these issues see a very accessible account by Boolos [Boo94].

sets, have a logical flavour in which we can interpret conjunction, possibly negation, quantification, and even perhaps sets membership, just as we have in this paper.

The treatment of universal quantification using the \mathbb{U} -quantifier and the notion of generous naming of internal sets (Definition 8.1) suggests a ‘new’ approach to impredicativity: it remains to abstract this from the specific application to NF, either for its own sake as a general theory, or as a technique to be explored and applied to other impredicative systems.

This paper proves consistency by building a concrete model; there is no formal consideration of what abstract class of structures that model belongs to. For instance, we can reasonably declare that our model should solve the equality $\mathcal{M} = pset(\mathcal{M})$ for some category and some meaning of $pset$ —and it then remains to examine the model for clues to what these should be. This is an opportunity particularly since many ways may exist to abstract the concrete model depending on what parts of its structure we consider important. For instance, the syntactic model of the simply-typed λ -calculus (terms quotiented by β -equivalence) can be generalised in at least three ways: to sets-and-functions, to Cartesian Closed Categories, and (noting that the confluence proof works without types, so perhaps they were not important) to domains.

Such a generalisation need not be specific to TST+ or NF, since our model is also a model of TST which is an important logic in its own right. Indeed, perhaps we should forget the set theory and just think about stratification and semantics of stratified (not necessarily ‘sets-flavoured’) languages. We can make this slightly more concrete: recall that we noted in the Introduction that stratification ensures that the rewrite $t \in \{a|\phi\} \rightarrow \phi[a:=t]$ terminates with a normal form containing only subterms of the form $t \in a$. This looks like a sets syntax, but that changes if we merely recast the syntax as $(\lambda a.s)t \rightarrow s[a:=t]$ and at .

13.2. Key ideas of this paper

We review some of the key ideas underlying the maths in this paper. In this discussion we try to be intuitive and brief (and not rigorous and strict in our use of our notation):

- (1) The ‘internal syntax’ of predicates and sets consists intuitively of normal forms under the rewrite $y \in \{a|\phi\} \rightarrow \phi[a \mapsto y]$. The stratification of TST+ is what guarantees normal forms. This allows us to write $p \models y \in a \Leftrightarrow y \in a \in p$ in Figure 3 (**modatm**). That is, points are sets of normal forms.
- (2) We take $\text{Set} = [\mathbb{A}]\text{Pred} = \text{Set}$ in syntax (Definition 3.1) and semantics (Figure 3 (**modset**) and Notation 8.6). This is *nominal atoms-abstraction*.
- (3) We import sigma- and amgis-actions from nominal duality theory to give semantics to predicates. Theorem 5.17 is particularly important.
- (4) We decompose \forall into ‘ \mathbb{U} ’ + ‘generous naming of atoms’ + ‘generous naming of sets’. Universal quantification is dangerous to us because of its impredicativity, and it takes some care to build up enough structure at each stage of this decomposition that we can move on to the next.
- (5) We focus on equality theories and the construction of ext (Definition 11.19).
- (6) We use an interesting technical device of the *Herbrand prepoint* (Definition 10.18). This definition seems natural, but at closer inspection also looks rather odd. It is not obvious that this should be a fruitful thing to look at, but it is.
- (7) The final construction of a point mixes the amgis-action and maximally consistent sets of predicates in a delicate way. See the exposition opening Section 12, and Remark 12.53.
- (8) The notion of ‘generous naming’ in Definition 8.1 is carefully designed, and as noted in Remark 8.2 is contingent not only on the point p and the internal set u , but also on the predicate X .

This makes it weaker (and so easier to handle) than a condition that $\partial a.p = p[x \leftarrow a]$.

This paper features two recursive constructions: that of ext in Definition 11.19 and another of $maxfilt(\Theta)$ in Definition 12.37 (whose definition, note, uses ext). Why two? Because we are solving

two distinct issues: the first is getting extensionality to work, the second is getting universal quantification to work.

While it may—or may not—be possible to unify these two recursions cleanly, keeping them separate can be viewed as a feature and not a bug; there may be other logics where we do not want extensionality (or perhaps want a weaker notion of extensionality), and (less plausibly, but not unreasonably) there may be logics where we do not want universal quantification (or perhaps want a weaker form of it). The proof in this paper is modular in such concerns; a non-modular proof, if one exists, is future work.

13.3. More on the use of nominal techniques

We sketch some specific technical uses of nominal techniques in this paper:

- (1) In Lemma 10.27, insisting on small support cuts down on the size of the powerset. This is discussed in Remark 10.28.
- (2) The notion of *small set of atoms* of Notation 2.6 is larger than the ‘small=finite’ of the original works on nominal techniques [GP99; GP01]. Notation 2.6 specifies a notion of smallness which
 - (a) is closed under taking powersets (a property that ‘small=finite’ also has), and
 - (b) permits small yet infinite sets of atoms.
 Property 2b above is required specifically for clause iib of the proof of Proposition 11.30.
- (3) We model universal quantification using the new-quantifier on sets from Definition 2.54, and we use the New and Generous quantifiers (\mathbb{N} and \mathbb{D}) from Definition 2.34 to reason about them. Their key properties go back to Lemma 2.11 and Theorem 2.39; the reader can consider Lemmas 8.11, 8.16, and the quantifier cases in Propositions 7.5 and 7.6, to see the style of reasoning enabled by these design choices.
- (4) Figure 3 (modal1) uses \mathbb{N} in an essential manner to specify the meaning of quantification, and Definition 8.3 uses \mathbb{D} in an essential manner to specify points. These two designs intersect in the proof of Lemma 8.14.
- (5) It seems to be important for the proofs that \mathbb{N} is ‘robust under small perturbations’. See the discussion in Remark 5.7.

We also use nominal techniques in two convenient but non-essential ways:

- (6) We use Equivariance (Theorem 2.31), which asserts the symmetry of atoms under permutation. Also Theorem 9.28 uses the symmetry of \mathbb{Z} under translation, which is another manifestation of the same idea. These results make proofs shorter—sometimes much shorter. Each specific application of equivariance can in principle be replaced by a longer inductive argument.²⁸
- (7) Similarly, we use nominal atoms-abstraction in Definition 3.1. That is, Definition 3.1 is nominal abstract syntax in the sense of [GP01]. This makes proofs shorter, but we could represent binding in other ways. We need nominal techniques anyway, so it is natural to use them for our syntax here.

The reader might ask whether nominal techniques are really necessary in this paper? Now that we know NF is consistent, and now that we have the structure of a working proof to dissect, could we re-engineer this proof to not use nominal techniques?

Doing this might yield a more accessible presentation, provided that the cost of this re-engineering does not unreasonably complicate the material. This remains to be seen.

It may be possible to modify the proof so that the use of nominal techniques is disguised, postponed, or avoided entirely. We certainly do not have to use nominal abstract syntax and we could avoid equivariance in inductive proofs (especially if we are willing to ‘hand-wave’ renaming properties instead of using results like Theorems 2.31 and 2.39). Modelling \forall using \mathbb{N} in Figure 3 is extremely

²⁸Consider this analogy: we can prove $n * m = m * n$ for numbers n and m by a vivid diagrammatic argument based on a rotation through ninety degrees. This general principle can be verified for a finite number of specific instances by a concrete calculation—‘counting pebbles’—but this is slower, less general, and inelegant.

convenient and may even be unavoidable—see the discussions in Remarks 5.7 and 5.20. The nominal ‘counting subsets’ lemmas of Subsection 10.6 are involved with building a ϑ -ambiguous model of TST, which is necessarily core to the consistency of NF.

However, from the point of view of this paper, such questions are perhaps not so important. If this proof is examined and found to be necessarily nominal then that will be very interesting, and if a non-nominal variant is discovered then that will also be very interesting. Either way, this is future work whose outcome will give us further perspective on the mathematics presented here. And, either way—looking now beyond NF—this paper uses a novel approach to logical semantics to good effect, as did previous work [Gab16; GG16]. We can ask to what other problems the method can be applied. This is also future work.

REFERENCES

- [Bar84] Henk P. Barendregt, *The lambda calculus: its syntax and semantics (revised ed.)*, North-Holland, 1984.
- [Bar14] *Barendregt’s substitution lemma*, June 2014, <http://isabelle.in.tum.de/nominal/example.html>, retrieved 2014/June/8.
- [Boo94] George Boolos, *Gödel’s second incompleteness theorem explained in words of one syllable*, *Mind* (1994), 1–3.
- [Che06] James Cheney, *Completeness and Herbrand theorems for nominal logic*, *Journal of Symbolic Logic* **71** (2006), 299–320.
- [Der87] Nachum Dershowitz, *Termination of rewriting*, *Journal of symbolic computation* **3** (1987), no. 1, 69–115.
- [DG12a] Gilles Dowek and Murdoch J. Gabbay, *Nominal Semantics for Predicate Logic: Algebras, Substitution, Quantifiers, and Limits*, *Proceedings of the 9th Italian Convention on Computational Logic (CILC 2012)*, CEUR workshop proceedings, vol. 857, 2012.
- [DG12b] ———, *Permissive Nominal Logic (journal version)*, *Transactions on Computational Logic* **13** (2012), no. 3.
- [DGM09] Gilles Dowek, Murdoch J. Gabbay, and Dominic P. Mulligan, *Permissive Nominal Terms and their Unification*, *Proceedings of the 24th Italian Conference on Computational Logic (CILC’09)*, 2009.
- [FG05] Maribel Fernández and Murdoch J. Gabbay, *Nominal rewriting with name generation: abstraction vs. locality*, *Proceedings of the 7th ACM SIGPLAN International Symposium on Principles and Practice of Declarative Programming (PPDP 2005)*, ACM Press, July 2005, pp. 47–58.
- [For95] Thomas E. Forster, *Set theory with a universal set: exploring an untyped universe*, Clarendon Press, 1995.
- [For97] ———, *Quine’s NF, 60 years on*, *American Mathematical Monthly* **104** (1997), no. 9, 838–845.
- [Fra22] Abraham Fraenkel, *Der Begriff “definit” und die Unabhängigkeit des Auswahlaxioms*, *Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse* (1922), 253–257, Reprinted in English translation in “From Frege to Gödel: A source book in mathematical logic 1879 - 1931”, Harvard University Press, second edition, 1971.
- [Gab01] Murdoch J. Gabbay, *A Theory of Inductive Definitions with alpha-Equivalence*, Ph.D. thesis, University of Cambridge, UK, March 2001.
- [Gab03] ———, *The pi-calculus in FM*, *Thirty-five years of Automating Mathematics* (Fairouz Kamareddine, ed.), Kluwer applied logic series, vol. 28, Kluwer, November 2003, pp. 247–269.
- [Gab07] ———, *A General Mathematics of Names*, *Information and Computation* **205** (2007), no. 7, 982–1011.

- [Gab09] ———, *A study of substitution, using nominal techniques and Fraenkel-Mostowski sets*, Theoretical Computer Science **410** (2009), no. 12-13, 1159–1189.
- [Gab11] ———, *Foundations of nominal techniques: logic and semantics of variables in abstract syntax*, Bulletin of Symbolic Logic **17** (2011), no. 2, 161–229.
- [Gab12] ———, *Finite and infinite support in nominal algebra and logic: nominal completeness theorems for free*, Journal of Symbolic Logic **77** (2012), no. 3.
- [Gab13] ———, *Nominal terms and nominal logics: from foundations to meta-mathematics*, Handbook of Philosophical Logic, vol. 17, Kluwer, 2013, (author's/publisher's numbering).
- [Gab14] ———, *Stone duality for First-Order Logic: a nominal approach*, HOWARD-60. A Festschrift on the Occasion of Howard Barringer's 60th Birthday, Easychair books, 2014.
- [Gab16] ———, *Semantics out of context: nominal absolute denotations for first-order logic and computation*, Journal of the ACM (2016), In press. See also arXiv preprint arxiv.org/abs/1305.6291.
- [GG10] Michael J. Gabbay and Murdoch J. Gabbay, *A simple class of Kripke-style models in which logic and computation have equal standing*, International Conference on Logic for Programming Artificial Intelligence and Reasoning (LPAR 2010), 2010.
- [GG16] Murdoch J. Gabbay and Michael J. Gabbay, *Representation and duality of the untyped lambda-calculus in nominal lattice and topological semantics, with a proof of topological completeness*, Annals of Pure and Applied Logic (2016), In press (submitted 2012). See also arXiv preprint 1305.5968.
- [GLP11] Murdoch J. Gabbay, Tadeusz Litak, and Daniela Petrişan, *Stone duality for nominal Boolean algebras with NEW*, Proceedings of the 4th international conference on algebra and coalgebra in computer science (CALCO 2011), Lecture Notes in Computer Science, vol. 6859, Springer, 2011, pp. 192–207.
- [GM06] Murdoch J. Gabbay and Aad Mathijssen, *Capture-avoiding Substitution as a Nominal Algebra*, Proceedings of the 3rd International Colloquium on Theoretical Aspects of Computing (ICTAC 2006) (Berlin), Lecture Notes in Computer Science, vol. 4281, Springer, November 2006, pp. 198–212.
- [GM08] ———, *Capture-Avoiding Substitution as a Nominal Algebra*, Formal Aspects of Computing **20** (2008), no. 4-5, 451–479.
- [GM09] ———, *Nominal universal algebra: equational logic with names and binding*, Journal of Logic and Computation **19** (2009), no. 6, 1455–1508.
- [GP99] Murdoch J. Gabbay and Andrew M. Pitts, *A New Approach to Abstract Syntax Involving Binders*, Proceedings of the 14th Annual Symposium on Logic in Computer Science (LICS 1999), IEEE Computer Society Press, July 1999, pp. 214–224.
- [GP01] ———, *A New Approach to Abstract Syntax with Variable Binding*, Formal Aspects of Computing **13** (2001), no. 3–5, 341–363.
- [Gri04] Nicholas Griffin, *The Prehistory of Russell's Paradox*, One Hundred Years of Russell's Paradox (Godehard Link, ed.), Series in Logic and Its Applications, no. 6, De Gruyter, 2004.
- [HG98] Paul R. Halmos and Steven Givant, *Logic as algebra*, Dolciani Mathematical Expositions, no. 21, Mathematical Association of America, 1998.
- [Hol98] Randall Holmes, *Elementary set theory with a universal set*, vol. 10, Centre National de recherches de Logique, 1998.
- [Jec06] Thomas Jech, *Set theory*, Springer, 2006, Third edition.
- [Joh03] Peter T. Johnstone, *Sketches of an elephant: A topos theory compendium*, Oxford Logic Guides, vol. 43 and 44, OUP, 2003.
- [KW96] Edward Keenan and Dag Westerståhl, *Generalized quantifiers in linguistics and logic*, Handbook of Logic and Language (J. Van Benthem and A. Ter Meulen, eds.), Elsevier, 1996, pp. 837–894.
- [MM92] Saunders Mac Lane and Ieke Moerdijk, *Sheaves in geometry and logic: A first introduction to topos theory*, Universitext, Springer, 1992.

- [Pit13] Andrew M. Pitts, *Nominal sets: Names and symmetry in computer science*, Cambridge University Press, May 2013.
- [Qui37] Willard V Quine, *New foundations for mathematical logic*, American mathematical monthly **4** (1937), no. 2, 70–80.
- [Spe58] Ernst Specker, *Dualität*, Dialectica **12** (1958), no. 3-4, 451–465.
- [Spe62] Ernst P Specker, *Typical ambiguity*, Logic Methodology and Philosophy of Science (Ernst Nagel, ed.), Stanford University Press, 1962, pp. 116–124.
- [Wad89] Philip Wadler, *Theorems for free!*, Proceedings of the 4th International Conference on Functional Programming Languages and Computer Architecture, ACM, 1989, pp. 347–359.
- [Wan81] Hao Wang, *Specker's mathematical work from 1949 to 1979*, L'Enseignement Mathématique **27** (1981), no. 1-2, <http://dx.doi.org/10.5169/seals-51741>.
- [Wes89] Dag Westerståhl, *Quantifiers in formal and natural languages*, Handbook of Philosophical Logic, Synthèse, vol. 4, Reidel, 1989, pp. 1–131.
- [Wil70] Stephen Willard, *General topology*, Addison Wesley, 1970.

A. A LITTLE MORE ON ELEMENTS AND LEIBNIZ EQUALITY

We discussed extensionality in Subsection 8.3, culminating with Theorem 8.20 which expressed that $x=x'$ should imply $Z[a \mapsto x] \Leftrightarrow Z[a \mapsto x']$. However, a more explicitly ‘sets-flavoured’ is that

$$\forall c. (a \in c \Leftrightarrow a' \in c) \quad \text{if and only if} \quad \forall b. (b \in a \Leftrightarrow b \in a').$$

It is quite interesting to work through the calculations needed to verify this directly.

Proposition A.1 reverses the implication of Theorem 8.20 (which is not hard), and this allows us to note an equality of denotations in Corollary A.2.

PROPOSITION A.1. *Suppose $i \in \mathbb{Z}$ and $a, a' \in \mathbb{A}^i$ and $b \in \mathbb{A}^{i-1}$ and $c \in \mathbb{A}^{i+1}$. Then (using Notation 6.1)*

$$[\forall a. \forall a'. (\forall c. (a \in c \Leftrightarrow a' \in c)) \Rightarrow (\forall b. (b \in a \Leftrightarrow b \in a'))] = \text{Pnt}.$$

Proof. Using Lemma 8.11(2) and Notations 6.1 and 8.18 with Lemma 5.9, it suffices to prove

$$[\forall c. (a \in c \Leftrightarrow a' \in c)] \subseteq [\forall b. (b \in a \Leftrightarrow b \in a')].$$

So suppose $p \in \text{Pnt}$ and $p \in [\forall c. (a \in c \Leftrightarrow a' \in c)]$.

Using Theorem 8.15 with Lemma 6.6(1) and Notations 6.1 and 8.18 with Lemma 5.9 we see that it suffices to prove that

- if $\forall w \in \text{Set}^{i+1}. p \in [a \in w] \Leftrightarrow p \in [a' \in w]$, then
- for any $v \in \text{Set}^{i-1}$, $p \in [v \in a] \Leftrightarrow p \in [v \in a']$.

Choose some $v \in \text{Set}^{i-1}$ and choose a fresh $c \in \mathbb{A}^i$ (so $c \# v, w$) and take in particular $w = [c](v \in c)$. The result follows by Corollary 6.7 (since $c \# v$). \square

COROLLARY A.2. *Continuing the notation of Proposition A.1 and using Notation 6.1,*

$$[\forall c. (a \in c \Leftrightarrow a' \in c)] = [\forall b. (b \in a \Leftrightarrow b \in a')].$$

Proof. From Theorem 8.20 and Proposition A.1. \square

B. THERE ARE INFINITELY MANY INTERNAL SETS AT EACH LEVEL

We now explicitly construct, at least in outline, a model of arithmetic in our model. This is possible in principle because we have translated TST+ to internal sets and predicates and thus given it a denotation (Figure 8 and Definition 9.14), but we now show some of the relevant concrete calculations.

NOTATION B.1. Suppose $i \in \mathbb{Z}$ and $x \in \text{Set}^{i-2}$. Choose fresh $c \in \mathbb{A}^{i-1}$ (so $c \# x$). Define $\text{contains}(x) \in \text{Set}^i$ by

$$\text{contains}(x) = [c] \text{elt}(x, c).$$

DEFINITION B.2. Suppose $i \in \mathbb{Z}$ and recall empt^i from Definition 3.11. Extend this definition to $\text{num}(n)^i$ for all $n \geq 0$ as follows:

$$\begin{aligned} \text{num}(0)^i &= \text{empt}^i \\ \text{num}(n)^i &= \text{contains}(\text{num}(n-1)^{i-2}) \quad n > 0 \end{aligned}$$

REMARK B.3. Intuitively, 0 corresponds to \emptyset and $n+1$ corresponds to $\{a \mid n \in a\}$.

LEMMA B.4. If $i \in \mathbb{Z}$ and $n \geq 0$ then:

- (1) $\text{num}(n)^i \in \text{Set}^i$.
- (2) $\text{supp}(\text{num}(n)^i) = \emptyset$.

Proof. By a routine induction on n . □

DEFINITION B.5. Suppose $i \in \mathbb{Z}$ and $x, y \in \text{Set}^i$ and suppose $c \in \mathbb{A}^{i-1}$ is fresh (so $c \# x, y$). Then we write

- We call x and y **coextensional** when $\llbracket \text{all}[c] \text{ iff}(x@c, y@c) \rrbracket = \text{Pnt}$.
- We call x and y **non-coextensional** when $\llbracket \text{all}[c] \text{ iff}(x@c, y@c) \rrbracket \subsetneq \text{Pnt}$.

We now prove that $\{\text{num}(n)^i \mid n \geq 0\}$ is an infinite set of non-coextensional internal sets, for every $i \in \mathbb{Z}$:

PROPOSITION B.6. Suppose $i \in \mathbb{Z}$ and $m, n \geq 0$. Then $\text{num}(n)^i$ and $\text{num}(m)^i$ are coextensional if and only if $n = m$.

Proof. We prove that $\text{num}(n)^i$ is coextensional with $\text{num}(n)^i$: by Definition B.5 and Lemma 8.11(2) it suffices to prove $\llbracket \text{iff}(\text{num}(n)^i@c, \text{num}(n)^i@c) \rrbracket = \text{Pnt}$ for some $c \in \mathbb{A}^{i-1}$. This is clear from Lemma 5.9.

We now prove by induction on $n + m$ that if $\text{num}(n)^i$ and $\text{num}(m)^i$ are coextensional then $n = m$. There are various cases:

- *The case that $n=0$ and $m>0$.* Choose $c \in \mathbb{A}^{i-1}$ and note by Lemma 8.11(2) and Lemma 5.9 that it suffices to exhibit a point p that is in $\llbracket \text{num}(m)^i@c \rrbracket$ and not in $\llbracket \text{num}(0)^i@c \rrbracket$. In fact by Lemmas 3.13(1) and 5.9(3) $\llbracket \text{num}(0)^i@c \rrbracket = \emptyset$, so we just need to exhibit a point in $\llbracket \text{num}(m)^i@c \rrbracket$. We unpack Definition B.2 and see that $\llbracket \text{num}(m)^i@c \rrbracket = \llbracket \text{elt}(\text{num}(m-1)^{i-2}, c) \rrbracket$. It suffices to take p to be any point where, applying a permutation if necessary, we assume $p(c) = p(\text{set}^{i-1})$ (following Definition 8.3 we can say c names set^{i-1} in p).
- *The case that $n>0$ and $m=0 \dots$* is symmetric with the previous case.
- *The case that $m=m'+1$ and $n=n'+1$.* From Definition B.2 and Lemma 2.66(1),

$$\llbracket \text{num}(m'+1)^i@c \rrbracket = \llbracket \text{elt}(\text{num}(m')^{i-2}, c) \rrbracket \quad \text{and} \quad \llbracket \text{num}(n'+1)^i@c \rrbracket = \llbracket \text{elt}(\text{num}(n')^{i-2}, c) \rrbracket.$$

It suffices to exhibit a point p that is in one but not the other.

By inductive hypothesis there exists a p such that $p \in \llbracket \text{num}(m')^{i-2}@c' \rrbracket$ and $p \notin \llbracket \text{num}(n')^{i-2}@c' \rrbracket$, or $p \notin \llbracket \text{num}(m')^{i-2}@c' \rrbracket$ and $p \in \llbracket \text{num}(n')^{i-2}@c' \rrbracket$, where $c' \in \mathbb{A}^{i-3}$. Without loss of generality assume the former.

Since p is a point we may assume, combining clauses 1 and 2 of Definition 8.3 and applying a permutation if necessary, that $p = p[[d] \text{elt}(c', d) \leftarrow c]$, where $d \in \mathbb{A}^{i-2}$ and $\text{elt}(c', d)$ is short for $\text{elt}(\text{atm}(c'), d)$. We will now prove that $p \in \llbracket \text{elt}(\text{num}(m')^{i-2}, c) \rrbracket$ and $p \notin \llbracket \text{elt}(\text{num}(n')^{i-2}, c) \rrbracket$.

Note by Lemma B.4(2) that $c, c' \# \text{num}(m')^{i-2}$ and by Theorem 2.31 $d \# \text{atm}(c')$:

$$\begin{aligned}
p &\in [\text{elt}(\text{num}(m')^{i-2}, c)] \\
&\Leftrightarrow c \circ \text{num}(m')^{i-2} \in p[[d] \text{elt}(c', d) \leftarrow c] && \text{Figure 3(modelt)} \\
&\Leftrightarrow p \in [([d] \text{elt}(c', d)) @ d][d \mapsto \text{num}(m')^{i-2}][c \mapsto [d] \text{elt}(c', d)]] && \text{Figure 4(}\tau\text{a)} \\
&\Leftrightarrow p \in [([d] \text{elt}(c', d)) @ d][d \mapsto \text{num}(m')^{i-2}]] && \text{Lemma 4.9 } c \# \text{num}(m')^{i-2} \\
&\Leftrightarrow p \in [\text{elt}(c', d)[d \mapsto \text{num}(m')^{i-2}]] && \text{Lemma 2.66(1)} \\
&\Leftrightarrow p \in [(\text{num}(m')^{i-2} @ c')[c' \mapsto \text{atm}(c')][d \mapsto \text{num}(m')^{i-2}]] && \text{Figure 1(}\sigma\text{elta)} \ c' \# \text{num}(m')^{i-2} \\
&\Leftrightarrow p \in [(\text{num}(m')^{i-2} @ c')[c' \mapsto \text{atm}(c')]] && \text{Lemma 4.9 } d \# \text{atm}(c') \\
&\Leftrightarrow p \in [\text{num}(m')^{i-2} @ c'] && \text{Lemma 4.16} \\
&\Leftrightarrow \top && \text{Assumption}
\end{aligned}$$

By similar reasoning we deduce that $p \in [\text{elt}(\text{num}(n')^{i-2}, c)] \Leftrightarrow \perp$, so we are done. \square